CISA
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
DEFEND TODAY, SECURE TOMORROW

Vulnerability Summary for the Week of October 25, 2021

Cybersecurity and Infrastructure Security Agency sent this bulletin at 11/01/2021 02:19 PM EDT

CISA
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
DEFEND TODAY, SECURE TOMORROW

You are subscribed to National Cyber Awareness System Bulletins for Cybersecurity and Infrastructure Security Agency. This information has recently been updated, and is now available.

Vulnerability Summary for the Week of October 25, 2021

11/01/2021 06:47 AM EDT

Original release date: November 1, 2021

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- storm	An Unsafe Deserialization vulnerability exists in the worker services of the Apache Storm supervisor server allowing pre-auth Remote Code Execution (RCE). Apache Storm 2.2.x users should upgrade to version 2.2.1 or 2.3.0. Apache Storm 2.1.x users should upgrade to version 2.1.1. Apache Storm 1.x users should upgrade to version 1.2.4	2021-10-25	7.5	CVE-2021-40865 MISC MISC
apache -- storm	A Command Injection vulnerability exists in the getTopologyHistory service of the Apache Storm 2.x prior to 2.2.1 and Apache Storm 1.x prior to 1.2.4. A specially crafted thrift request to the Nimbus server allows Remote Code Execution (RCE) prior to authentication.	2021-10-25	7.5	CVE-2021-38294 MISC MISC
auvesy -- versiondog	The scheduler service running on a specific TCP port enables the user to start and stop jobs. There is no sanitation of the supplied JOB ID provided to the function. An attacker may send a malicious payload that can enable the user to execute another SQL expression by sending a specific string.	2021-10-22	7.5	CVE-2021-38481 CONFIRM
auvesy -- versiondog	The data of a network capture of the initial handshake phase can be used to authenticate at a SYSDBA level. If a specific .exe is not restarted often, it is possible to access the needed handshake packets between admin/client connections. Using the SYSDBA permission, an attacker can change user passwords or delete the database.	2021-10-22	7.5	CVE-2021-38459 CONFIRM
auvesy -- versiondog	The server permits communication without any authentication procedure, allowing the attacker to initiate a session with the server without providing any form of authentication.	2021-10-22	7.5	CVE-2021-38457 CONFIRM
auvesy -- versiondog	The database connection to the server is performed by calling a specific API, which could allow an unprivileged user to gain SYSDBA permissions.	2021-10-22	9	CVE-2021-38475 CONFIRM
auvesy -- versiondog	Some API functions permit by-design writing or copying data into a given buffer. Since the client controls these parameters, an attacker could rewrite the memory in any location of the affected product.	2021-10-22	7.5	CVE-2021-38449 CONFIRM
cct95 -- chichen_tech_cms	Chichen Tech CMS v1.0 was discovered to contain multiple SQL injection vulnerabilities in the file product_list.php via the id and cid parameters.	2021-10-22	10	CVE-2020-28960 MISC

Subscribe to updates from Cybersecu Infrastructure Security Agency

Email Address e.g. name

Subscribe

Share Bulletin

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
checkpoint -- harmony_browse	The Harmony Browse and the SandBlast Agent for Browsers installers must have admin privileges to execute some steps during the installation. Because the MS Installer allows regular users to repair their installation, an attacker running an installer before 90.08.7405 can start the installation repair and place a specially crafted binary in the repair folder, which runs with the admin privileges.	2021-10-22	7.2	CVE-2021-30359 MISC MISC
cisco -- adaptive_security_appliance	A vulnerability in SSL/TLS message handler for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because incoming SSL/TLS packets are not properly processed. An attacker could exploit this vulnerability by sending a crafted SSL/TLS packet to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.	2021-10-27	7.8	CVE-2021-40117 CISCO
cisco -- adaptive_security_appliance	Multiple vulnerabilities in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. These vulnerabilities are due to improper input validation when parsing HTTPS requests. An attacker could exploit these vulnerabilities by sending a malicious HTTPS request to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.	2021-10-27	7.1	CVE-2021-40118 CISCO
cisco -- adaptive_security_appliance	A vulnerability in the software-based SSL/TLS message handler of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient validation of SSL/TLS messages when the device performs software-based SSL/TLS decryption. An attacker could exploit this vulnerability by sending a crafted SSL/TLS message to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. Note: Datagram TLS (DTLS) messages cannot be used to exploit this vulnerability.	2021-10-27	7.8	CVE-2021-34783 CISCO
cisco -- adaptive_security_appliance	A vulnerability in the memory management of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper resource management when connection rates are high. An attacker could exploit this vulnerability by opening a significant number of connections on an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.	2021-10-27	7.8	CVE-2021-34792 CISCO
cisco -- firepower_management_center	Multiple Cisco products are affected by a vulnerability in the way the Snort detection engine processes ICMP traffic that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper memory resource management while the Snort detection engine is processing ICMP packets. An attacker could exploit this vulnerability by sending a series of ICMP packets through an affected device. A successful exploit could allow the attacker to exhaust resources on the affected device, causing the device to reload.	2021-10-27	7.8	CVE-2021-40114 CISCO
cisco -- firepower_management_center	Multiple Cisco products are affected by a vulnerability in Snort rules that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.The vulnerability is due to improper handling of the Block with Reset or Interactive Block with Reset actions if a rule is configured without proper constraints. An attacker could exploit this vulnerability by sending a crafted IP packet to the affected device. A successful exploit could allow the attacker to cause through traffic to be dropped. Note: Only products with Snort3 configured and either a rule with Block with Reset or Interactive Block with Reset actions configured are vulnerable. Products configured with Snort2 are not vulnerable.	2021-10-27	7.1	CVE-2021-40116 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- firepower_management_center_virtual_appliance	A vulnerability in the processing of SSH connections for multi-instance deployments of Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on the affected device. This vulnerability is due to a lack of proper error handling when an SSH session fails to be established. An attacker could exploit this vulnerability by sending a high rate of crafted SSH connections to the instance. A successful exploit could allow the attacker to cause resource exhaustion, which causes a DoS condition on the affected device. The device must be manually reloaded to recover.	2021-10-27	7.1	CVE-2021-34781 CISCO
cisco -- firepower_management_center_virtual_appliance	Multiple vulnerabilities in the CLI of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. For more information about these vulnerabilities, see the Details section of this advisory.	2021-10-27	7.2	CVE-2021-34756 CISCO
cisco -- firepower_management_center_virtual_appliance	Multiple vulnerabilities in the CLI of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. For more information about these vulnerabilities, see the Details section of this advisory.	2021-10-27	7.2	CVE-2021-34755 CISCO
cszcms -- csz_cms	CSZ CMS v1.2.4 was discovered to contain an arbitrary file upload vulnerability in the component /core/MY_Security.php.	2021-10-27	7.5	CVE-2020-21250 MISC
eclipse -- openj9	In Eclipse Openj9 before version 0.29.0, the JVM does not throw IllegalAccessError for MethodHandles that invoke inaccessible interface methods.	2021-10-25	7.5	CVE-2021-41035 CONFIRM CONFIRM CONFIRM
flashget -- flashget	FlashGet v1.9.6 was discovered to contain a buffer overflow in the 'current path directory' function. This vulnerability allows attackers to elevate local process privileges via overwriting the registers.	2021-10-22	9	CVE-2020-28967 MISC
gestionaleopen -- gestionale_open	An Insecure Permissions issue exists in Gestionale Open 11.00.00. A low privilege account is able to rename the mysqld.exe file located in bin folder and replace with a malicious file that would connect back to an attacking computer giving system level privileges (nt authority\system) due to the service running as Local System. While a low privilege user is unable to restart the service through the application, a restart of the computer triggers the execution of the malicious file. The application also have unquoted service path issues.	2021-10-26	9.3	CVE-2021-37363 MISC MISC
google -- android	In ccu, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594996; Issue ID: ALPS05594996.	2021-10-25	7.2	CVE-2021-0625 MISC
google -- android	In display driver, there is a possible memory corruption due to uninitialized data. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05594994; Issue ID: ALPS05594994.	2021-10-25	7.2	CVE-2021-0634 MISC
google -- android	In RW_SetActivatedTagType of rw_main.cc, there is possible memory corruption due to a race condition. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-192472262	2021-10-22	9.3	CVE-2021-0870 MISC MISC
google -- android	In bpf_skb_change_head of filter.c, there is a possible out of bounds read due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-154177719References: Upstream kernel	2021-10-25	7.2	CVE-2021-0941 MISC
google -- android	In TBD of TBD, there is a possible out of bounds write due to improper locking. This could lead to local escalation of privilege in the kernel with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-171315276References: N/A	2021-10-25	7.2	CVE-2021-0940 MISC
google -- android	In ip6_xmit of ip6_output.c, there is a possible out of bounds write due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-168607263References: Upstream kernel	2021-10-25	7.2	CVE-2021-0935 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In runDumpHeap of ActivityManagerShellCommand.java, there is a possible deletion of system files due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-183262161	2021-10-22	7.2	CVE-2021-0708 MISC
google -- android	In sanitizeSbn of NotificationManagerService.java, there is a possible way to keep service running in foreground and keep granted permissions due to Bypass of Background Service Restrictions. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-10Android ID: A-185388103	2021-10-22	7.2	CVE-2021-0705 MISC
google -- android	In SecondStageMain of init.cpp, there is a possible use after free due to incorrect shared_ptr usage. This could lead to local escalation of privilege if the attacker has physical access to the device, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-184569329	2021-10-22	7.2	CVE-2021-0703 MISC
google -- android	In audio DSP, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05844458; Issue ID: ALPS05844458.	2021-10-25	7.2	CVE-2021-0663 MISC
google -- android	In audio DSP, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05844434; Issue ID: ALPS05844434.	2021-10-25	7.2	CVE-2021-0662 MISC
google -- android	In VectorDrawable::VectorDrawable of VectorDrawable.java, there is a possible way to introduce a memory corruption due to sharing of not thread-safe objects. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-185178568	2021-10-22	7.2	CVE-2021-0652 MISC
google -- android	In audio DSP, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05844413; Issue ID: ALPS05844413.	2021-10-25	7.2	CVE-2021-0661 MISC
google -- android	In display driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05585423; Issue ID: ALPS05585423.	2021-10-25	7.2	CVE-2021-0633 MISC
gridprosoftware -- request_management	Gridpro Request Management for Windows Azure Pack before 2.0.7912 allows Directory Traversal for remote code execution, as demonstrated by ..\ in a scriptName JSON value to ServiceManagerTenant/GetVisibilityMap.	2021-10-25	7.5	CVE-2021-40371 MISC MISC MISC
huawei -- imanager_neteco_6000_firmware	There is a signature management vulnerability in some huawei products. An attacker can forge signature and bypass the signature check. During firmware update process, successful exploit this vulnerability can cause the forged system file overwrite the correct system file. Affected product versions include:iManager NetEco V600R010C00CP2001,V600R010C00CP2002,V600R010C00SPC100,V600R010C00SPC110,V600R010C00SPC120 NetEco 6000 V600R009C00SPC100,V600R009C00SPC110,V600R009C00SPC120,V600R009C00SPC190,V600R009C00SPC20	2021-10-27	9	CVE-2021-37127 MISC
inria -- caml-light	caml-light <= 0.75 uses mktemp() insecurely, and also does unsafe things in /tmp during make install.	2021-10-26	7.5	CVE-2011-4119 MISC MISC MISC
krylack -- zip_password_recovery	Passcovery Co. Ltd ZIP Password Recovery v3.70.69.0 was discovered to contain a buffer overflow via the decompress function.	2021-10-22	7.2	CVE-2020-28963 MISC
mcafee -- total_protection	Privilege escalation vulnerability in the Windows trial installer of McAfee Total Protection (MTP) prior to 16.0.34_x may allow a local user to run arbitrary code as the admin user by replacing a specific temporary file created during the installation of the trial version of MTP.	2021-10-26	7.2	CVE-2021-23877 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
online_student_admission_system_project -- online_student_admission_system	Online Student Admission System 1.0 is affected by an unauthenticated SQL injection bypass vulnerability in /admin/login.php.	2021-10-26	7.5	CVE-2021-37371 MISC MISC MISC
openclinic_ga_project -- openclinic_ga	OpenClinic GA 5.194.18 is affected by Insecure Permissions. By default the Authenticated Users group has the modify permission to openclinic folders/files. A low privilege account is able to rename mysqld.exe or tomcat8.exe files located in bin folders and replace with a malicious file that would connect back to an attacking computer giving system level privileges (nt authority\system) due to the service running as Local System. While a low privilege user is unable to restart the service through the application, a restart of the computer triggers the execution of the malicious file. The application also have unquoted service path issues.	2021-10-26	9.3	CVE-2021-37364 MISC MISC MISC
openpowerfoundation -- skiboot	An issue was discovered in OpenPOWER 2.6 firmware. unpack_timestamp() calls le32_to_cpu() for endian conversion of a uint16_t "year" value, resulting in a type mismatch that can truncate a higher integer value to a smaller one, and bypass a timestamp check. The fix is to use the right endian conversion function.	2021-10-22	7.5	CVE-2021-36357 MISC
parallels -- parallels_desktop	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 16.1.3 (49160). An attacker must first obtain the ability to execute low-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the Toolgate component. The issue results from the lack of proper validation of user-supplied data, which can result in an uncontrolled memory allocation. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-13544.	2021-10-25	7.2	CVE-2021-34854 N/A N/A
php -- php	In PHP versions 7.3.x up to and including 7.3.31, 7.4.x below 7.4.25 and 8.0.x below 8.0.12, when running PHP FPM SAPI with main FPM daemon process running as root and child worker processes running as lower-privileged users, it is possible for the child processes to access memory shared with the main process and write to it, modifying it in a way that would cause the root process to conduct invalid memory reads and writes, which can be used to escalate privileges from local unprivileged user to the root user.	2021-10-25	7.2	CVE-2021-21703 MISC DEBIAN DEBIAN MLIST MLIST FEDORA FEDORA
polarssl -- polarssl	PolarSSL versions prior to v1.1 use the HAVEGE random number generation algorithm. At its heart, this uses timing information based on the processor's high resolution timer (the RDTSC instruction). This instruction can be virtualized, and some virtual machine hosts have chosen to disable this instruction, returning 0s or predictable results.	2021-10-27	7.5	CVE-2011-4574 MISC
portable -- playable	Portable Ltd Playable v9.18 contains a code injection vulnerability in the filename parameter, which allows attackers to execute arbitrary web scripts or HTML via a crafted POST request.	2021-10-22	7.5	CVE-2020-23037 MISC
salesagility -- suitecrm	SuiteCRM before 7.11.19 allows remote code execution via the system settings Log File Name setting. In certain circumstances involving admin account takeover, logger_file_name can refer to an attacker-controlled PHP file under the web root, because only the all-lowercase PHP file extensions were blocked. NOTE: this issue exists because of an incomplete fix for CVE-2020-28328.	2021-10-22	9	CVE-2021-42840 MISC MISC MISC MISC
showdoc -- showdoc	ShowDoc 2.8.3 ihas a file upload vulnerability, where attackers can use the vulnerability to obtain server permissions.	2021-10-22	7.5	CVE-2021-41745 MISC MISC
simple_payroll_system_with_dynamic_tax_bracket_project -- simple_payroll_system_with_dynamic_tax_bracket	The Simple Payroll System with Dynamic Tax Bracket in PHP using SQLite Free Source Code (by: oretnom23) is vulnerable from remote SQL-Injection-Bypass-Authentication for the admin account. The parameter (username) from the login form is not protected correctly and there is no security and escaping from malicious payloads.	2021-10-22	7.5	CVE-2021-42169 MISC
sixapart -- movable_type	Movable Type 7 r.5002 and earlier (Movable Type 7 Series), Movable Type 6.8.2 and earlier (Movable Type 6 Series), Movable Type Advanced 7 r.5002 and earlier (Movable Type Advanced 7 Series), Movable Type Advanced 6.8.2 and earlier (Movable Type Advanced 6 Series), Movable Type Premium 1.46 and earlier, and Movable Type Premium Advanced 1.46 and earlier allow remote attackers to execute arbitrary OS commands via unspecified vectors. Note that all versions of Movable Type 4.0 or later including unsupported (End-of-Life, EOL) versions are also affected by this vulnerability.	2021-10-26	7.5	CVE-2021-20837 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
solarwinds -- kiwi_cattools	As a result of an unquoted service path vulnerability present in the Kiwi CatTools Installation Wizard, a local attacker could gain escalated privileges by inserting an executable into the path of the affected service or uninstall entry.	2021-10-22	7.2	CVE-2021-35230 MISC
sourcecodester -- complaint_management_system	An SQL Injection vulnerability exists in Sourcecodester Complaint Management System 1.0 via the cid parameter in complaint-details.php.	2021-10-27	7.5	CVE-2020-24932 MISC
tonec -- internet_download_manager	Internet Download Manager 6.37.11.1 was discovered to contain a stack buffer overflow in the Search function. This vulnerability allows attackers to escalate local process privileges via unspecified vectors.	2021-10-22	7.2	CVE-2020-28964 MISC
websvn -- websvn	A flaw was found in WebSVN 2.3.2. Without prior authentication, if the 'allowDownload' option is enabled in config.php, an attacker can invoke the dl.php script and pass a well formed 'path' argument to execute arbitrary commands against the underlying operating system.	2021-10-26	9.3	CVE-2011-2195 MISC
yonyou -- ufida_product_lifecycle_management	All versions of yongyou PLM are affected by a command injection issue. UFIDA PLM (Product Life Cycle Management) is a strategic management method. It applies a series of enterprise application systems to support the entire process from conceptual design to the end of product life, and the collaborative creation, distribution, application and management of product information across organizations. Yonyou PLM uses jboss by default, and you can access the management control background without authorization An attacker can use this vulnerability to gain server permissions.	2021-10-22	7.5	CVE-2021-41744 MISC

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
advantech -- webaccess\/nms	WebAccess/NMS (Versions prior to v3.0.3_Build6299) has an improper authentication vulnerability, which may allow unauthorized users to view resources monitored and controlled by the WebAccess/NMS, as well as IP addresses and names of all the devices managed via WebAccess/NMS.	2021-10-27	5	CVE-2021-32951 MISC
air_sender_project -- air_sender	Tran Tu Air Sender v1.0.2 was discovered to contain an arbitrary file upload vulnerability in the upload module. This vulnerability allows attackers to execute arbitrary code via a crafted file.	2021-10-22	6.5	CVE-2020-23043 MISC
anaconda -- dask	An issue was discovered in Dask (aka python-dask) through 2021.09.1. Single machine Dask clusters started with dask.distributed.LocalCluster or dask.distributed.Client (which defaults to using LocalCluster) would mistakenly configure their respective Dask workers to listen on external interfaces (typically with a randomly selected high port) rather than only on localhost. A Dask cluster created using this method (when running on a machine that has an applicable port exposed) could be used by a sophisticated attacker to achieve remote code execution.	2021-10-26	6.8	CVE-2021-42343 MISC
aplixio -- pdf_shapingup	Aplioxio PDF ShapingUp 5.0.0.139 contains a buffer overflow which allows attackers to cause a denial of service (DoS) via a crafted PDF file.	2021-10-22	6.8	CVE-2020-28969 MISC
atlassian -- jira	Affected versions of Atlassian Jira Server and Data Center allow authenticated yet non-administrator remote attackers to edit the File Replication settings via a Broken Access Control vulnerability in the `ReplicationSettings!default.jspa` endpoint. The affected versions are before version 8.6.0, from version 8.7.0 before 8.13.12, and from version 8.14.0 before 8.20.1.	2021-10-26	4	CVE-2021-41308 MISC
atlassian -- jira	Affected versions of Atlassian Jira Server and Data Center allow anonymous remote attackers to view the names of private projects and filters via an Insecure Direct Object References (IDOR) vulnerability in the Average Number of Times in Status Gadget. The affected versions are before version 8.13.12..	2021-10-26	5	CVE-2021-41305 MISC
atlassian -- jira	Affected versions of Atlassian Jira Server and Data Center allow anonymous remote attackers to view private project and filter names via an Insecure Direct Object References (IDOR) vulnerability in the Average Time in Status Gadget. The affected versions are before version 8.13.12, and from version 8.14.0 before 8.20.0.	2021-10-26	5	CVE-2021-41306 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
atlassian -- jira	Affected versions of Atlassian Jira Server and Data Center allow unauthenticated remote attackers to view the names of private projects and private filters via an Insecure Direct Object References (IDOR) vulnerability in the Workload Pie Chart Gadget. The affected versions are before version 8.13.12, and from version 8.14.0 before 8.20.0.	2021-10-26	5	CVE-2021-41307 MISC
atlassian -- jira	Affected versions of Atlassian Jira Server and Data Center allow anonymous remote attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability in the /secure/admin/ImporterFinishedPage.jspa error message. The affected versions are before version 8.13.12, and from version 8.14.0 before 8.20.1.	2021-10-26	4.3	CVE-2021-41304 MISC
automatedlogic -- webctrl	The login portal for the Automated Logic WebCTRL/WebCTRL OEM web application contains a vulnerability that allows for reflected XSS attacks due to the operatorlocale GET parameter not being sanitized. This issue impacts versions 6.5 and below. This issue works by passing in a basic XSS payload to a vulnerable GET parameter that is reflected in the output without sanitization.	2021-10-22	4.3	CVE-2021-31682 MISC MISC MISC
auvesy -- versiondog	Many API function codes receive raw pointers remotely from the user and trust these pointers as valid in-bound memory regions. An attacker can manipulate API functions by writing arbitrary data into the resolved address of a raw pointer.	2021-10-22	5	CVE-2021-38479 CONFIRM
auvesy -- versiondog	A specific function code receives a raw pointer supplied by the user and deallocates this pointer. The user can then control what memory regions will be freed and cause use-after-free condition.	2021-10-22	5.5	CVE-2021-38467 CONFIRM
auvesy -- versiondog	The affected product does not properly control the allocation of resources. A user may be able to allocate unlimited memory buffers using API functions.	2021-10-22	5.5	CVE-2021-38463 CONFIRM
auvesy -- versiondog	There are multiple API function codes that permit data writing to any file, which may allow an attacker to modify existing files or create new files.	2021-10-22	6.4	CVE-2021-38471 CONFIRM
auvesy -- versiondog	The affected product uses a hard-coded blowfish key for encryption/decryption processes. The key can be easily extracted from binaries.	2021-10-22	6.4	CVE-2021-38461 CONFIRM
auvesy -- versiondog	Some API functions allow interaction with the registry, which includes reading values as well as data modification.	2021-10-22	6.4	CVE-2021-38453 CONFIRM
auvesy -- versiondog	There are multiple API function codes that permit reading and writing data to or from files and directories, which could lead to the manipulation and/or the deletion of files.	2021-10-22	6.4	CVE-2021-38477 CONFIRM
auvesy -- versiondog	The affected product's code base doesn't properly control arguments for specific functions, which could lead to a stack overflow.	2021-10-22	6.5	CVE-2021-38473 CONFIRM
auvesy -- versiondog	The affected product's OS Service does not verify any given parameter. A user can supply any type of parameter that will be passed to inner calls without checking the type of the parameter or the value.	2021-10-22	4	CVE-2021-38455 CONFIRM
auvesy -- versiondog	The webinstaller is a Golang web server executable that enables the generation of an Auvesy image agent. Resource consumption can be achieved by generating large amounts of installations, which are then saved without limitation in the temp folder of the webinstaller executable.	2021-10-22	4	CVE-2021-38465 CONFIRM
auvesy -- versiondog	Many of the services used by the affected product do not specify full paths for the DLLs they are loading. An attacker can exploit the uncontrolled search path by implanting their own DLL near the affected product's binaries, thus hijacking the loaded DLL.	2021-10-22	4.3	CVE-2021-38469 CONFIRM
bqe -- billquick_web_suite	BQE BillQuick Web Suite 2018 through 2021 before 22.0.9.1 allows SQL injection for unauthenticated remote code execution, as exploited in the wild in October 2021 for ransomware installation. SQL injection can, for example, use the txtID (aka username) parameter. Successful exploitation can include the ability to execute arbitrary code as MSSQLSERVER$ via xp_cmdshell.	2021-10-22	6.8	CVE-2021-42258 MISC
cisco -- adaptive_security_appliance	Multiple vulnerabilities in the Application Level Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the ALG and open unauthorized connections with a host located behind the ALG. For more information about these vulnerabilities, see the Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT Slipstreaming.	2021-10-27	5	CVE-2021-34790 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- adaptive_security_appliance	A vulnerability in the identity-based firewall (IDFW) rule processing feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass security protections. This vulnerability is due to improper handling of network requests by affected devices configured to use object group search. An attacker could exploit this vulnerability by sending a specially crafted network request to an affected device. A successful exploit could allow the attacker to bypass access control list (ACL) rules on the device, bypass security protections, and send network traffic to unauthorized hosts.	2021-10-27	4.3	CVE-2021-34787 CISCO
cisco -- adaptive_security_appliance	Multiple vulnerabilities in the Application Level Gateway (ALG) for the Network Address Translation (NAT) feature of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the ALG and open unauthorized connections with a host located behind the ALG. For more information about these vulnerabilities, see the Details section of this advisory. Note: These vulnerabilities have been publicly discussed as NAT Slipstreaming.	2021-10-27	5	CVE-2021-34791 CISCO
cisco -- adaptive_security_appliance	A vulnerability in the TCP Normalizer of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software operating in transparent mode could allow an unauthenticated, remote attacker to poison MAC address tables, resulting in a denial of service (DoS) vulnerability. This vulnerability is due to incorrect handling of certain TCP segments when the affected device is operating in transparent mode. An attacker could exploit this vulnerability by sending a crafted TCP segment through an affected device. A successful exploit could allow the attacker to poison the MAC address tables in adjacent devices, resulting in network disruption.	2021-10-27	5	CVE-2021-34793 CISCO
cisco -- adaptive_security_appliance	A vulnerability in the Simple Network Management Protocol version 3 (SNMPv3) access control functionality of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to query SNMP data. This vulnerability is due to ineffective access control. An attacker could exploit this vulnerability by sending an SNMPv3 query to an affected device from a host that is not permitted by the SNMPv3 access control list. A successful exploit could allow the attacker to send an SNMP query to an affected device and retrieve information from the device. The attacker would need valid credentials to perform the SNMP query.	2021-10-27	5	CVE-2021-34794 CISCO
cisco -- adaptive_security_appliance	A vulnerability in the Internet Key Exchange Version 2 (IKEv2) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to trigger a denial of service (DoS) condition on an affected device. This vulnerability is due to improper control of a resource. An attacker with the ability to spoof a trusted IKEv2 site-to-site VPN peer and in possession of valid IKEv2 credentials for that peer could exploit this vulnerability by sending malformed, authenticated IKEv2 messages to an affected device. A successful exploit could allow the attacker to trigger a reload of the device.	2021-10-27	6.3	CVE-2021-40125 CISCO
cisco -- firepower_management_center	Multiple vulnerabilities in the payload inspection for Ethernet Industrial Protocol (ENIP) traffic for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass configured rules for ENIP traffic. These vulnerabilities are due to incomplete processing during deep packet inspection for ENIP packets. An attacker could exploit these vulnerabilities by sending a crafted ENIP packet to the targeted interface. A successful exploit could allow the attacker to bypass configured access control and intrusion policies that should be activated for the ENIP packet.	2021-10-27	5	CVE-2021-34754 CISCO
cisco -- firepower_management_center_virtual_appliance	A vulnerability in Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to overwrite or append arbitrary data to system files using root-level privileges. The attacker must have administrative credentials on the device. This vulnerability is due to incomplete validation of user input for a specific CLI command. An attacker could exploit this vulnerability by authenticating to the device with administrative privileges and issuing a CLI command with crafted user parameters. A successful exploit could allow the attacker to overwrite or append arbitrary data to system files using root-level privileges.	2021-10-27	6.6	CVE-2021-34761 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- firepower_management_center_virtual_appliance	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an attacker to execute a cross-site scripting (XSS) attack or an open redirect attack. For more information about these vulnerabilities, see the Details section of this advisory.	2021-10-27	5.8	CVE-2021-34764 CISCO
cisco -- firepower_management_center_virtual_appliance	A vulnerability in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to perform a directory traversal attack on an affected device. The attacker would require valid device credentials. The vulnerability is due to insufficient input validation of the HTTPS URL by the web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTPS request that contains directory traversal character sequences to an affected device. A successful exploit could allow the attacker to read or write arbitrary files on the device.	2021-10-27	5.5	CVE-2021-34762 CISCO
cloudfoundry -- capi-release	Cloud Controller versions prior to 1.118.0 are vulnerable to unauthenticated denial of Service(DoS) vulnerability allowing unauthenticated attackers to cause denial of service by using REST HTTP requests with label_selectors on multiple V3 endpoints by generating an enormous SQL query.	2021-10-27	5	CVE-2021-22101 MISC
codesys -- codesys	In the CODESYS V2 web server prior to V1.1.9.22 crafted web server requests may cause a Null pointer dereference in the CODESYS web server and may result in a denial-of-service condition.	2021-10-26	5	CVE-2021-34586 CONFIRM MISC
codesys -- codesys	In the CODESYS V2 web server prior to V1.1.9.22 crafted web server requests can trigger a parser error. Since the parser result is not checked under all conditions, a pointer dereference with an invalid address can occur. This leads to a denial of service situation.	2021-10-26	5	CVE-2021-34585 CONFIRM MISC
codesys -- codesys	Crafted web server requests may cause a heap-based buffer overflow and could therefore trigger a denial-of- service condition due to a crash in the CODESYS V2 web server prior to V1.1.9.22.	2021-10-26	5	CVE-2021-34583 CONFIRM MISC
codesys -- codesys	Crafted web server requests can be utilised to read partial stack or heap memory or may trigger a denial-of- service condition due to a crash in the CODESYS V2 web server prior to V1.1.9.22.	2021-10-26	6.4	CVE-2021-34584 CONFIRM MISC
codesys -- plcwinnt	A crafted request with invalid offsets may cause an out-of-bounds read or write access in CODESYS V2 Runtime Toolkit 32 Bit full and PLCWinNT prior to versions V2.4.7.56, resulting in a denial-of-service condition or local memory overwrite.	2021-10-26	5.5	CVE-2021-34595 CONFIRM
codesys -- plcwinnt	In CODESYS V2 Runtime Toolkit 32 Bit full and PLCWinNT prior to versions V2.4.7.56 unauthenticated crafted invalid requests may result in several denial-of-service conditions. Running PLC programs may be stopped, memory may be leaked, or further communication clients may be blocked from accessing the PLC.	2021-10-26	5	CVE-2021-34593 CONFIRM FULLDISC
codesys -- plcwinnt	A crafted request may cause a read access to an uninitialized pointer in CODESYS V2 Runtime Toolkit 32 Bit full and PLCWinNT prior to versions V2.4.7.56, resulting in a denial-of-service condition.	2021-10-26	4	CVE-2021-34596 CONFIRM
csdn -- csdn_app	Cross-Site Scripting (XSS) vulnerability exists in Csdn APP 4.10.0, which can be exploited by attackers to obtain sensitive information such as user cookies.	2021-10-22	4.3	CVE-2021-41747 MISC MISC
customer_relationship_management_system_project -- customer_relationship_management_system	A file upload vulnerability exists in Sourcecodester Customer Relationship Management System 1.0 via the account update option & customer create option, which could let a remote malicious user upload an arbitrary php file. .	2021-10-27	6.5	CVE-2021-37221 MISC
d-link -- dap-2020_firmware	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2020 1.01rc001 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the var:page parameter provided to the webproc endpoint. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-13271.	2021-10-25	5.8	CVE-2021-34863 N/A N/A
d-link -- dap-2020_firmware	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2020 1.01rc001 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the var:menu parameter provided to the webproc endpoint. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-13270.	2021-10-25	5.8	CVE-2021-34862 N/A N/A

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
d-link -- dap-2020_firmware	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2020 1.01rc001 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the webproc endpoint, which listens on TCP port 80 by default. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-12104.	2021-10-25	5.8	CVE-2021-34861 N/A N/A
dedecms -- dedecms	DedeCMS v7.5 SP2 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities in the component makehtml_homepage.php via the `filename`, `mid`, `userid`, and `templet' parameters.	2021-10-22	4.3	CVE-2020-36497 MISC
dedecms -- dedecms	DedeCMS v7.5 SP2 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities in the component tpl.php via the `filename`, `mid`, `userid`, and `templet' parameters.	2021-10-22	4.3	CVE-2020-23046 MISC
dedecms -- dedecms	DedeCMS v7.5 SP2 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities in the component mychannel_edit.php via the `filename`, `mid`, `userid`, and `templet' parameters.	2021-10-22	4.3	CVE-2020-36494 MISC
dedecms -- dedecms	DedeCMS v7.5 SP2 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities in the component file_manage_view.php via the `filename`, `mid`, `userid`, and `templet' parameters.	2021-10-22	4.3	CVE-2020-36495 MISC
dedecms -- dedecms	DedeCMS v7.5 SP2 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities in the component sys_admin_user_edit.php via the `filename`, `mid`, `userid`, and `templet' parameters.	2021-10-22	4.3	CVE-2020-36496 MISC
dropouts -- air_share	Dropouts Technologies LLP Air Share v1.2 was discovered to contain a cross-site scripting (XSS) vulnerability in the path parameter of the `list` and `download` exception-handling. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted GET request.	2021-10-22	4.3	CVE-2020-23041 MISC
dropouts -- super_backup	Dropouts Technologies LLP Super Backup v2.0.5 was discovered to contain a cross-site scripting (XSS) vulnerability in the path parameter of the `list` and `download` module. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted GET request.	2021-10-22	4.3	CVE-2020-23042 MISC
dropouts -- super_backup	Dropouts Technologies LLP Super Backup v2.0.5 was discovered to contain an issue in the path parameter of the `list` and `download` module which allows attackers to perform a directory traversal via a change to the path variable to request the local list command.	2021-10-22	5	CVE-2020-23061 MISC
elabftw -- elabftw	eLabFTW is an open source electronic lab notebook manager for research teams. In versions of eLabFTW before 4.1.0, it allows attackers to bypass a brute-force protection mechanism by using many different forged PHPSESSID values in HTTP Cookie header. This issue has been addressed by implementing brute force login protection, as recommended by Owasp with Device Cookies. This mechanism will not impact users and will effectively thwart any brute-force attempts at guessing passwords. The only correct way to address this is to upgrade to version 4.1.0. Adding rate limitation upstream of the eLabFTW service is of course a valid option, with or without upgrading.	2021-10-22	4	CVE-2021-41171 CONFIRM MISC MISC MISC MISC
emerson -- wireless_1410_gateway_firmware	The affected product is vulnerable to a disclosure of peer username and password by allowing all users access to read global variables.	2021-10-22	4	CVE-2021-42536 CONFIRM
emerson -- wireless_1410_gateway_firmware	The affected product is vulnerable to directory traversal due to mishandling of provided backup folder structure.	2021-10-22	6.5	CVE-2021-42542 CONFIRM
emerson -- wireless_1410_gateway_firmware	The affected product is vulnerable to a unsanitized extract folder for system configuration. A low-privileged user can leverage this logic to overwrite the settings and other key functionality.	2021-10-22	6.5	CVE-2021-42540 CONFIRM
emerson -- wireless_1410_gateway_firmware	The affected product is vulnerable to improper input validation in the restore file. This enables an attacker to provide malicious config files to replace any file on disk.	2021-10-22	6.5	CVE-2021-38485 CONFIRM
emerson -- wireless_1410_gateway_firmware	The affected product is vulnerable to a parameter injection via passphrase, which enables the attacker to supply uncontrolled input.	2021-10-22	6.5	CVE-2021-42538 CONFIRM
emerson -- wireless_1410_gateway_firmware	The affected product is vulnerable to a missing permission validation on system backup restore, which could lead to account take over and unapproved settings change.	2021-10-22	6.5	CVE-2021-42539 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
facebook -- hhvm	HHVM supports the use of an "admin" server which accepts administrative requests over HTTP. One of those request handlers, dump-pcre-cache, can be used to output cached regular expressions from the current execution context into a file. The handler takes a parameter which specifies where on the filesystem to write this data. The parameter is not validated, allowing a malicious user to overwrite arbitrary files where the user running HHVM has write access. This issue affects HHVM versions prior to 4.56.2, all versions between 4.57.0 and 4.78.0, as well as 4.79.0, 4.80.0, 4.81.0, 4.82.0, and 4.83.0.	2021-10-26	5.5	CVE-2019-3556 CONFIRM CONFIRM CONFIRM
firefly-iii -- firefly_iii	firefly-iii is vulnerable to Cross-Site Request Forgery (CSRF)	2021-10-27	4.3	CVE-2021-3900 MISC CONFIRM
freeswitch -- freeswitch	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. By default, SIP requests of the type SUBSCRIBE are not authenticated in the affected versions of FreeSWITCH. Abuse of this security issue allows attackers to subscribe to user agent event notifications without the need to authenticate. This abuse poses privacy concerns and might lead to social engineering or similar attacks. For example, attackers may be able to monitor the status of target SIP extensions. Although this issue was fixed in version v1.10.6, installations upgraded to the fixed version of FreeSWITCH from an older version, may still be vulnerable if the configuration is not updated accordingly. Software upgrades do not update the configuration by default. SIP SUBSCRIBE messages should be authenticated by default so that FreeSWITCH administrators do not need to explicitly set the `auth-subscriptions` parameter. When following such a recommendation, a new parameter can be introduced to explicitly disable authentication.	2021-10-26	5	CVE-2021-41157 CONFIRM MISC MISC FULLDISC
freeswitch -- freeswitch	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to version 1.10.7, an attacker can perform a SIP digest leak attack against FreeSWITCH and receive the challenge response of a gateway configured on the FreeSWITCH server. This is done by challenging FreeSWITCH's SIP requests with the realm set to that of the gateway, thus forcing FreeSWITCH to respond with the challenge response which is based on the password of that targeted gateway. Abuse of this vulnerability allows attackers to potentially recover gateway passwords by performing a fast offline password cracking attack on the challenge response. The attacker does not require special network privileges, such as the ability to sniff the FreeSWITCH's network traffic, to exploit this issue. Instead, what is required for this attack to work is the ability to cause the victim server to send SIP request messages to the malicious party. Additionally, to exploit this issue, the attacker needs to specify the correct realm which might in some cases be considered secret. However, because many gateways are actually public, this information can easily be retrieved. The vulnerability appears to be due to the code which handles challenges in `sofia_reg.c`, `sofia_reg_handle_sip_r_challenge()` which does not check if the challenge is originating from the actual gateway. The lack of these checks allows arbitrary UACs (and gateways) to challenge any request sent by FreeSWITCH with the realm of the gateway being targeted. This issue is patched in version 10.10.7. Maintainers recommend that one should create an association between a SIP session for each gateway and its realm to make a check be put into place for this association when responding to challenges.	2021-10-26	5	CVE-2021-41158 CONFIRM MISC FULLDISC
freeswitch -- freeswitch	Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. FreeSWITCH prior to version 1.10.7 is susceptible to Denial of Service via SIP flooding. When flooding FreeSWITCH with SIP messages, it was observed that after a number of seconds the process was killed by the operating system due to memory exhaustion. By abusing this vulnerability, an attacker is able to crash any FreeSWITCH instance by flooding it with SIP messages, leading to Denial of Service. The attack does not require authentication and can be carried out over UDP, TCP or TLS. This issue was patched in version 1.10.7.	2021-10-25	5	CVE-2021-41145 CONFIRM MISC FULLDISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
freeswitch -- freeswitch	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. When handling SRTP calls, FreeSWITCH prior to version 1.10.7 is susceptible to a DoS where calls can be terminated by remote attackers. This attack can be done continuously, thus denying encrypted calls during the attack. When a media port that is handling SRTP traffic is flooded with a specially crafted SRTP packet, the call is terminated leading to denial of service. This issue was reproduced when using the SDES key exchange mechanism in a SIP environment as well as when using the DTLS key exchange mechanism in a WebRTC environment. The call disconnection occurs due to line 6331 in the source file `switch_rtp.c`, which disconnects the call when the total number of SRTP errors reach a hard-coded threshold (100). By abusing this vulnerability, an attacker is able to disconnect any ongoing calls that are using SRTP. The attack does not require authentication or any special foothold in the caller's or the callee's network. This issue is patched in version 1.10.7.	2021-10-25	5	CVE-2021-41105 CONFIRM MISC FULLDISC
froala -- wysiwyg-editor	A cross site scripting (XSS) vulnerability in the Insert Video function of Froala WYSIWYG Editor 3.1.0 allows attackers to execute arbitrary web scripts or HTML.	2021-10-26	4.3	CVE-2020-22864 MISC MISC
game-server-status_project -- game-server-status	The Game Server Status WordPress plugin through 1.0 does not validate or escape the server_id parameter before using it in SQL statement, leading to an Authenticated SQL Injection in an admin page	2021-10-25	6.5	CVE-2021-24662 MISC
gjson_project -- gjson	GJSON before 1.9.3 allows a ReDoS (regular expression denial of service) attack.	2021-10-22	5	CVE-2021-42836 MISC MISC MISC MISC MISC
google -- android	In multiple methods of AAudioService, there is a possible use-after-free due to a race condition. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11Android ID: A-153358911	2021-10-22	4.4	CVE-2021-0483 MISC
google -- android	In acc_read of f_accessory.c, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-173789633References: Upstream kernel	2021-10-25	4.6	CVE-2021-0936 MISC
google -- android	In loadLabel of PackageItemInfo.java, there is a possible way to DoS a device by having a long label in an app due to incorrect input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11 Android-9 Android-10Android ID: A-67013844	2021-10-22	4.7	CVE-2021-0651 MISC
google -- android	In startListening of PluginManagerImpl.java, there is a possible way to disable arbitrary app components due to a missing permission check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-193444889	2021-10-22	4.9	CVE-2021-0706 MISC
google -- android	In wifi driver, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05551397; Issue ID: ALPS05551397.	2021-10-25	5	CVE-2021-0630 MISC
google -- android	In wifi driver, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05551435; Issue ID: ALPS05551435.	2021-10-25	5	CVE-2021-0631 MISC
helpu -- helpuviewer	An improper input validation vulnerability in Helpu solution could allow a local attacker to arbitrary file creation and execution without click file transfer menu. It is possible to file in arbitrary directory for user because the viewer program receive the file from agent with privilege of administrator.	2021-10-27	4.6	CVE-2020-7867 MISC
huawei -- emui	There is a Configuration defects in Huawei Smartphone.Successful exploitation of this vulnerability may affect service availability.	2021-10-28	5	CVE-2021-22405 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
huawei -- emui	There is a Directory traversal vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service confidentiality.	2021-10-28	5	CVE-2021-22404 MISC
huawei -- emui	There is a Remote DoS vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability can affect service integrity.	2021-10-28	5	CVE-2021-22401 MISC
huawei -- emui	There is a DoS vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause DoS attacks.	2021-10-28	5	CVE-2021-22402 MISC
huawei -- fusioncube_firmware	There is a path traversal vulnerability in Huawei FusionCube 6.0.2.The vulnerability is due to that the software uses external input to construct a pathname that is intended to identify a directory that is located underneath a restricted parent directory, but the software does not properly validate the pathname. Successful exploit could allow the attacker to access a location that is outside of the restricted directory by a crafted filename.	2021-10-27	5	CVE-2021-37130 MISC
huawei -- ips_module_firmware	There is an out of bounds write vulnerability in some Huawei products. The vulnerability is caused by a function of a module that does not properly verify input parameter. Successful exploit could cause out of bounds write leading to a denial of service condition.Affected product versions include:IPS Module V500R005C00,V500R005C20;NGFW Module V500R005C00;NIP6600 V500R005C00,V500R005C20;S12700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600,V200R013C00SPC500,V200R019C00SPC20 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S2700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S5700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600,V200R019C00SPC50 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;S7700 V200R010C00SPC600,V200R010C00SPC700,V200R011C10SPC500,V200R011C10SPC600;S9700 V200R010C00SPC600,V200R011C10SPC500,V200R011C10SPC600;USG9500 V500R005C00,V500R005C20.	2021-10-27	5	CVE-2021-37129 MISC
huawei -- manageone	There is a CSV injection vulnerability in ManageOne, iManager NetEco and iManager NetEco 6000. An attacker with high privilege may exploit this vulnerability through some operations to inject the CSV files. Due to insufficient input validation of some parameters, the attacker can exploit this vulnerability to inject CSV files to the target device.	2021-10-27	6	CVE-2021-37131 MISC
ibm -- business_automation_workflow	IBM Business Automation Workflow 18.0, 19.0, 20.0, and 21.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204833.	2021-10-22	4.3	CVE-2021-29835 CONFIRM XF
ibm -- engineering_lifecycle_optimization	IBM Jazz Team Server products could allow an authenticated user to obtain elevated privileges under certain configurations. IBM X-Force ID: 203025.	2021-10-27	6	CVE-2021-29774 XF CONFIRM
ibm -- planning_analytics	IBM Planning Analytics 2.0 could allow a remote attacker to obtain sensitive information, caused by the failure to set the HTTPOnly flag. A remote attacker could exploit this vulnerability to obtain sensitive information from the cookie. IBM X-Force ID: 198755.	2021-10-27	5	CVE-2021-20526 CONFIRM XF
ingeteam -- ingepac_da_au_firmware	Ingeteam INGEPAC DA AU AUC_1.13.0.28 (and before) web application allows access to a certain path that contains sensitive information that could be used by an attacker to execute more sophisticated attacks. An unauthenticated remote attacker with access to the device´s web service could exploit this vulnerability in order to obtain different configuration files.	2021-10-25	5	CVE-2017-20007 CONFIRM
jquery -- jquery_ui	jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `altField` option of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `altField` option is now treated as a CSS selector. A workaround is to not accept the value of the `altField` option from untrusted sources.	2021-10-26	4.3	CVE-2021-41182 CONFIRM MISC MISC
jquery -- jquery_ui	jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of various `*Text` options of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. The values passed to various `*Text` options are now always treated as pure text, not HTML. A workaround is to not accept the value of the `*Text` options from untrusted sources.	2021-10-26	4.3	CVE-2021-41183 MISC MISC CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jquery -- jquery_ui	jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `of` option of the `.position()` util from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `of` option is now treated as a CSS selector. A workaround is to not accept the value of the `of` option from untrusted sources.	2021-10-26	4.3	CVE-2021-41184 MISC CONFIRM MISC
jquery-reply-to-comment_project -- jquery-reply-to-comment	The jQuery Reply to Comment WordPress plugin through 1.31 does not have any CSRF check when saving its settings, nor sanitise or escape its 'Quote String' and 'Reply String' settings before outputting them in Comments, leading to a Stored Cross-Site Scripting issue.	2021-10-25	4.3	CVE-2021-24543 MISC
kumilabs -- swift_file_transfer	Swift File Transfer Mobile v1.1.2 and below was discovered to contain an information disclosure vulnerability in the path parameter. This vulnerability is exploited via an error caused by including non-existent path environment variables.	2021-10-22	5	CVE-2020-23038 MISC
macs_cms_project -- macs_cms	Macrob7 Macs Framework Content Management System - 1.14f was discovered to contain a cross-site scripting (XSS) vulnerability in the search input field of the search module.	2021-10-22	4.3	CVE-2020-23047 MISC
macs_cms_project -- macs_cms	Macrob7 Macs Framework Content Management System - 1.14f was discovered to contain a SQL injection vulnerability via the 'roleId' parameter of the `editRole` and `deletUser` modules.	2021-10-22	6.5	CVE-2020-23045 MISC
madeportable -- playable	Portable Ltd Playable v9.18 was discovered to contain an arbitrary file upload vulnerability in the filename parameter of the upload module. This vulnerability allows attackers to execute arbitrary code via a crafted JPEG file.	2021-10-22	4.6	CVE-2020-36485 MISC
mangboard -- mang_board	A vulnerability was found in Mangboard(WordPress plugin). A SQL-Injection vulnerability was found in order_type parameter. The order_type parameter makes a SQL query using unfiltered data. This vulnerability allows a remote attacker to steal user information.	2021-10-26	5	CVE-2021-26609 MISC
mcafee -- epolicy_orchestrator	Cross-Site Scripting vulnerability in McAfee ePolicy Orchestrator (ePO) prior to 5.10 Update 11 allows ePO administrators to inject arbitrary web script or HTML via a specific parameter where the administrator's entries were not correctly sanitized.	2021-10-22	4.3	CVE-2021-31835 CONFIRM
medianavi -- smacom	MEDIA NAVI Inc SMACom v1.2 was discovered to contain an insecure session validation vulnerability in the session handling of the `password` authentication parameter of the wifi photo transfer module. This vulnerability allows attackers with network access privileges or on public wifi networks to read the authentication credentials and follow-up requests containing the user password via a man in the middle attack.	2021-10-22	4.3	CVE-2020-23036 MISC
mycodo_project -- mycodo	Mycodo is an environmental monitoring and regulation system. An exploit in versions prior to 8.12.7 allows anyone with access to endpoints to download files outside the intended directory. A patch has been applied and a release made. Users should upgrade to version 8.12.7. As a workaround, users may manually apply the changes from the fix commit.	2021-10-26	4	CVE-2021-41185 CONFIRM MISC MISC MISC
nameko -- nameko	Nameko through 2.13.0 can be tricked into performing arbitrary code execution when deserializing the config file.	2021-10-26	6.8	CVE-2021-41078 MISC MISC
nextcloud -- deck	Nextcloud is an open-source, self-hosted productivity platform. A missing permission check in Nextcloud Deck before 1.2.9, 1.4.5 and 1.5.3 allows another authenticated users to access Deck cards of another user. It is recommended that the Nextcloud Deck App is upgraded to 1.2.9, 1.4.5 or 1.5.3. There are no known workarounds aside from upgrading.	2021-10-25	5.5	CVE-2021-39225 CONFIRM MISC MISC
nextcloud -- nextcloud_server	Nextcloud is an open-source, self-hosted productivity platform. Prior to versions 20.0.13, 21.0.5, and 22.2.0, Nextcloud Server did not implement a database backend for rate-limiting purposes. Any component of Nextcloud using rate-limits (as as `AnonRateThrottle` or `UserRateThrottle`) was thus not rate limited on instances not having a memory cache backend configured. In the case of a default installation, this would notably include the rate-limits on the two factor codes. It is recommended that the Nextcloud Server be upgraded to 20.0.13, 21.0.5, or 22.2.0. As a workaround, enable a memory cache backend in `config.php`.	2021-10-25	5.5	CVE-2021-41177 CONFIRM MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nextcloud -- officeonline	Nextcloud is an open-source, self-hosted productivity platform. The Nextcloud OfficeOnline application prior to version 1.1.1 returned verbatim exception messages to the user. This could result in a full path disclosure on shared files. (e.g. an attacker could see that the file `shared.txt` is located within `/files/$username/Myfolder/Mysubfolder/shared.txt`). It is recommended that the OfficeOnline application is upgraded to 1.1.1. As a workaround, one may disable the OfficeOnline application in the app settings.	2021-10-25	5	CVE-2021-39224 CONFIRM MISC
nextcloud -- richdocuments	Nextcloud is an open-source, self-hosted productivity platform. The Nextcloud Richdocuments application prior to versions 3.8.6 and 4.2.3 returned verbatim exception messages to the user. This could result in a full path disclosure on shared files. (e.g. an attacker could see that the file `shared.txt` is located within `/files/$username/Myfolder/Mysubfolder/shared.txt`). It is recommended that the Richdocuments application is upgraded to 3.8.6 or 4.2.3. As a workaround, disable the Richdocuments application in the app settings.	2021-10-25	5	CVE-2021-39223 MISC CONFIRM MISC
nextcloud -- server	Nextcloud is an open-source, self-hosted productivity platform. Prior to versions 20.0.13, 21.0.5, and 22.2.0, a file traversal vulnerability makes an attacker able to download arbitrary SVG images from the host system, including user provided files. This could also be leveraged into a XSS/phishing attack, an attacker could upload a malicious SVG file that mimics the Nextcloud login form and send a specially crafted link to victims. The XSS risk here is mitigated due to the fact that Nextcloud employs a strict Content-Security-Policy disallowing execution of arbitrary JavaScript. It is recommended that the Nextcloud Server be upgraded to 20.0.13, 21.0.5 or 22.2.0. There are no known workarounds aside from upgrading.	2021-10-25	4	CVE-2021-41178 MISC MISC CONFIRM
nextcloud -- server	Nextcloud is an open-source, self-hosted productivity platform. Prior to Nextcloud Server versions 20.0.13, 21.0.5, and 22.2.0, the Two-Factor Authentication wasn't enforced for pages marked as public. Any page marked as `@PublicPage` could thus be accessed with a valid user session that isn't authenticated. This particularly affects the Nextcloud Talk application, as this could be leveraged to gain access to any private chat channel without going through the Two-Factor flow. It is recommended that the Nextcloud Server be upgraded to 20.0.13, 21.0.5 or 22.2.0. There are no known workarounds aside from upgrading.	2021-10-25	4	CVE-2021-41179 MISC MISC CONFIRM
nxp -- mcuxpresso_software_development_kit	NXP MCUXpresso SDK v2.7.0 was discovered to contain a buffer overflow in the function USB_HostProcessCallback().	2021-10-25	4.6	CVE-2021-38258 MISC
nxp -- mcuxpresso_software_development_kit	NXP MCUXpresso SDK v2.7.0 was discovered to contain a buffer overflow in the function USB_HostParseDeviceConfigurationDescriptor().	2021-10-25	4.6	CVE-2021-38260 MISC
onepeloton -- peloton	Exposure of senstive information to an unauthorised actor in the "com.onepeloton.erlich" mobile application up to and including version 1.7.22 allows a remote attacker to access developer files stored in an AWS S3 bucket, by reading credentials stored in plain text within the mobile application.	2021-10-25	5	CVE-2021-40527 CONFIRM
onepeloton -- ttr01_firmware	Incorrect calculation of buffer size vulnerability in Peleton TTR01 up to and including PTV55G allows a remote attacker to trigger a Denial of Service attack through the GymKit daemon process by exploiting a heap overflow in the network server handling the Apple GymKit communication. This can lead to an Apple MFI device not being able to authenticate with the Peleton Bike	2021-10-25	5	CVE-2021-40526 CONFIRM
online_student_admission_system_project -- online_student_admission_system	Online Student Admission System 1.0 is affected by an insecure file upload vulnerability. A low privileged user can upload malicious PHP files by updating their profile image to gain remote code execution.	2021-10-26	6.5	CVE-2021-37372 MISC MISC MISC
parallels -- parallels_desktop	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 16.1.3 (49160). An attacker must first obtain the ability to execute high-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the virtio-gpu virtual device. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-13581.	2021-10-25	4.6	CVE-2021-34856 N/A N/A

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
parallels -- parallels_desktop	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 16.1.3 (49160). An attacker must first obtain the ability to execute high-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the Toolgate component. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-13601.	2021-10-25	4.6	CVE-2021-34857 N/A N/A
parallels -- parallels_desktop	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 16.1.3 (49160). An attacker must first obtain the ability to execute low-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the WinAppHelper component. The issue results from the lack of proper access control. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-13543.	2021-10-25	4.6	CVE-2021-34864 N/A
permalink_manager_lite_project -- permalink_manager_lite	The Permalink Manager Lite WordPress plugin before 2.2.13.1 does not validate and escape the orderby parameter before using it in a SQL statement in the Permalink Manager page, leading to a SQL Injection	2021-10-25	6.5	CVE-2021-24769 MISC
pterodactyl -- panel	Pterodactyl is an open-source game server management panel built with PHP 7, React, and Go. In affected versions of Pterodactyl a malicious user can trigger a user logout if a signed in user visits a malicious website that makes a request to the Panel's sign-out endpoint. This requires a targeted attack against a specific Panel instance, and serves only to sign a user out. **No user details are leaked, nor is any user data affected, this is simply an annoyance at worst.** This is fixed in version 1.6.3.	2021-10-25	4.3	CVE-2021-41176 MISC CONFIRM MISC
rasa -- rasa_x	Rasa X before 0.42.4 allows Directory Traversal during archive extraction. In the functionality that allows a user to load a trained model archive, an attacker has arbitrary write capability within specific directories via a crafted archive file.	2021-10-22	4.3	CVE-2021-42556 MISC CONFIRM
sanskruti -- st-daily-tip	The St-Daily-Tip WordPress plugin through 4.7 does not have any CSRF check in place when saving its 'Default Text to Display if no tips' setting, and was also lacking sanitisation as well as escaping before outputting it the page. This could allow attacker to make logged in administrators set a malicious payload in it, leading to a Stored Cross-Site Scripting issue	2021-10-25	6.8	CVE-2021-24487 MISC
seeddms -- seeddms	SeedDMS Content Management System v6.0.7 contains a persistent cross-site scripting (XSS) vulnerability in the component AddEvent.php via the name and comment parameters.	2021-10-22	4.3	CVE-2020-23048 MISC
sky_file_project -- sky_file	Sky File v2.1.0 contains a directory traversal vulnerability in the FTP server which allows attackers to access sensitive data and files via 'null' path commands.	2021-10-22	5	CVE-2020-23040 MISC
sky_file_project -- sky_file	An issue in the FTP server of Sky File v2.1.0 allows attackers to perform directory traversal via `/null//` path commands.	2021-10-22	4	CVE-2020-36488 MISC
skyworth -- penguin_aurora_box_firmware	Penguin Aurora TV Box 41502 is a high-end network HD set-top box produced by Tencent Video and Skyworth Digital. An unauthorized access vulnerability exists in the Penguin Aurora Box. An attacker can use the vulnerability to gain unauthorized access to a specific link to remotely control the TV.	2021-10-26	6.4	CVE-2021-41873 MISC
solarwinds -- kiwi_syslog_server	The HTTP TRACK & TRACE methods were enabled in Kiwi Syslog Server 9.7.1 and earlier. These methods are intended for diagnostic purposes only. If enabled, the web server will respond to requests that use these methods by returning exact HTTP request that was received in the response to the client. This may lead to the disclosure of sensitive information such as internal authentication headers appended by reverse proxies.	2021-10-27	5	CVE-2021-35233 MISC MISC
solarwinds -- kiwi_syslog_server	As a result of an unquoted service path vulnerability present in the Kiwi Syslog Server Installation Wizard, a local attacker could gain escalated privileges by inserting an executable into the path of the affected service or uninstall entry. Example vulnerable path: "Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Kiwi Syslog Server\Parameters\Application".	2021-10-25	4.6	CVE-2021-35231 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
solarwinds -- kiwi_syslog_server	The ASP.NET debug feature is enabled by default in Kiwi Syslog Server 9.7.2 and previous versions. ASP.NET allows remote debugging of web applications, if configured to do so. Debug mode causes ASP.NET to compile applications with extra information. The information enables a debugger to closely monitor and control the execution of an application. If an attacker could successfully start a remote debugging session, this is likely to disclose sensitive information about the web application and supporting infrastructure that may be valuable in targeting SWI with malicious intent.	2021-10-27	5	CVE-2021-35235 MISC MISC
solarwinds -- kiwi_syslog_server	The Secure flag is not set in the SSL Cookie of Kiwi Syslog Server 9.7.2 and previous versions. The Secure attribute tells the browser to only send the cookie if the request is being sent over a secure channel such as HTTPS. This will help protect the cookie from being passed over unencrypted requests. If the application can be accessed over both HTTP, there is a potential for the cookie can be sent in clear text.	2021-10-27	5	CVE-2021-35236 MISC MISC
sourcecodester -- news247_cms	Cross Site Scripting (XSS) vulnerability exists in Sourcecodester News247 CMS 1.0 via the search function in articles.	2021-10-28	4.3	CVE-2021-41728 MISC
strategy11 -- formidable_form_builder	The Formidable Form Builder WordPress plugin before 4.09.05 allows to inject certain HTML Tags like <audio>,<video>,<img>,<a> and<button>.This could allow an unauthenticated, remote attacker to exploit a HTML-injection byinjecting a malicous link. The HTML-injection may trick authenticated users to follow the link. If the Link gets clicked, Javascript code can be executed. The vulnerability is due to insufficient sanitization of the "data-frmverify" tag for links in the web-based entry inspection page of affected systems. A successful exploitation incomibantion with CSRF could allow the attacker to perform arbitrary actions on an affected system with the privileges of the user. These actions include stealing the users account by changing their password or allowing attackers to submit their own code through an authenticated user resulting in Remote Code Execution. If an authenticated user who is able to edit Wordpress PHP Code in any kind, clicks the malicious link, PHP code can be edited.	2021-10-25	6.8	CVE-2021-24884 MISC MISC MISC
swiftfiletransfer -- swift_file_transfer	Swift File Transfer Mobile v1.1.2 was discovered to contain a cross-site scripting (XSS) vulnerability via the devicename parameter which allows attackers to execute arbitrary web scripts or HTML via a crafted payload entered as the device name itself.	2021-10-22	4.3	CVE-2020-36502 MISC
swiftfiletransfer -- swift_file_transfer	Swift File Transfer Mobile v1.1.2 and below was discovered to contain a cross-site scripting (XSS) vulnerability via the 'path' parameter of the 'list' and 'download' exception-handling.	2021-10-22	4.3	CVE-2020-36486 MISC
taotesting -- tao_assessment_platform	TAO Open Source Assessment Platform v3.3.0 RC02 was discovered to contain a HTML injection vulnerability in the userFirstName parameter of the user account input field. This vulnerability allows attackers to execute phishing attacks, external redirects, and arbitrary code.	2021-10-22	6	CVE-2020-23050 MISC
teamviewer -- teamviewer	This vulnerability allows remote attackers to execute arbitrary code on affected installations of TeamViewer 15.16.8.0. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of TVS files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13697.	2021-10-25	6.8	CVE-2021-34859 N/A N/A
tonec -- internet_download_manager	Internet Download Manager 6.37.11.1 was discovered to contain a stack buffer overflow in the Export/Import function. This vulnerability allows attackers to escalate local process privileges via a crafted ef2 file.	2021-10-22	6.6	CVE-2020-23060 MISC
trane -- tracer_concierge	The affected controllers do not properly sanitize the input containing code syntax. As a result, an attacker could craft code to alter the intended controller flow of the software.	2021-10-27	6.5	CVE-2021-38450 CONFIRM
trane -- tracer_sc_firmware	The affected product's web application does not properly neutralize the input during webpage generation, which could allow an attacker to inject code in the input forms.	2021-10-22	4.3	CVE-2021-42534 CONFIRM
user-agent_switcher_and_manager_project -- user-agent_switcher_and_manager	A cross-site scripting (XSS) vulnerability in NSK User Agent String Switcher Service v0.3.5 allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the user agent input field.	2021-10-22	4.3	CVE-2020-23054 MISC
user_registration_ amp;_login_and_user_management_system_with_admin_panel_project -- user_registration_ amp;_login_and_user_management_system_with_admin_panel	Phpgurukul User Registration & User Management System v2.0 was discovered to contain multiple stored cross-site scripting (XSS) vulnerabilities via the firstname and lastname parameters of the registration form & loginsystem input fields.	2021-10-22	4.3	CVE-2020-23051 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wp_debugging_project -- wp_debugging	The WP Debugging WordPress plugin before 2.11.0 has its update_settings() function hooked to admin_init and is missing any capability and CSRF checks, as a result, the settings can be updated by unauthenticated users.	2021-10-25	4.3	CVE-2021-24779 MISC
wpchill -- check_ amp;_log_email	The Check & Log Email WordPress plugin before 1.0.3 does not validate and escape the "order" and "orderby" GET parameters before using them in a SQL statement when viewing logs, leading to SQL injections issues	2021-10-25	6.5	CVE-2021-24774 MISC
yop-poll -- yop-poll	The YOP Poll WordPress plugin before 6.1.2 does not escape the perpage parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting	2021-10-25	4.3	CVE-2021-24885 CONFIRM MISC

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
akaunting -- akaunting	Akaunting v1.3.17 was discovered to contain a stored cross-site scripting (XSS) vulnerability which allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the Company Name input field.	2021-10-25	3.5	CVE-2020-20908 MISC
antsword_redis_project -- antsword_redis	AS_Redis is an AntSword plugin for Redis. The Redis Manage plugin for AntSword prior to version 0.5 is vulnerable to Self-XSS due to due to insufficient input validation and sanitization via redis server configuration. Self-XSS in the plugin configuration leads to code execution. This issue is patched in version 0.5.	2021-10-26	3.5	CVE-2021-41172 MISC CONFIRM MISC
auvesy -- versiondog	The affected product's proprietary protocol CSC allows for calling numerous function codes. In order to call those function codes, the user must supply parameters. There is no sanitation on the value of the offset, which allows the client to specify any offset and read out-of-bounds data.	2021-10-22	3.5	CVE-2021-38451 CONFIRM
catalyst -- mahara	Catalyst IT Ltd Mahara CMS v19.10.2 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities in the component groupfiles.php via the Number (Nombre) and Description (Descripción) parameters.	2021-10-22	3.5	CVE-2020-23052 MISC
cimatti -- contact_forms	The WordPress Contact Forms by Cimatti WordPress plugin before 1.4.12 does not sanitise and escape the Form Title before outputting it in some admin pages. which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed.	2021-10-25	3.5	CVE-2021-24744 MISC
cisco -- firepower_management_center_virtual_appliance	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an attacker to execute a cross-site scripting (XSS) attack or an open redirect attack. For more information about these vulnerabilities, see the Details section of this advisory.	2021-10-27	3.5	CVE-2021-34763 CISCO
cookie-bar_project -- cookie-bar	The Cookie Bar WordPress plugin through 1.8.8 doesn't properly sanitise the Cookie Bar Message setting, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	2021-10-25	3.5	CVE-2021-24653 MISC
d-link -- dap-2020_firmware	This vulnerability allows network-adjacent attackers to disclose sensitive information on affected installations of D-Link DAP-2020 1.01rc001 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the getpage parameter provided to the webproc endpoint. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-12103.	2021-10-25	3.3	CVE-2021-34860 N/A N/A
dedecms -- dedecms	DedeCMS v7.5 SP2 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities in the component file_pic_view.php via the `activepath`, `keyword`, `tag`, `fmdo=x&filename`, `CKEditor` and `CKEditorFuncNum` parameters.	2021-10-22	3.5	CVE-2020-23044 MISC
dedecms -- dedecms	DedeCMS v7.5 SP2 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities in the component file_manage_view.php via the `activepath`, `keyword`, `tag`, `fmdo=x&filename`, `CKEditor` and `CKEditorFuncNum` parameters.	2021-10-22	3.5	CVE-2020-36490 MISC
dedecms -- dedecms	DedeCMS v7.5 SP2 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities in the component media_main.php via the `activepath`, `keyword`, `tag`, `fmdo=x&filename`, `CKEditor` and `CKEditorFuncNum` parameters.	2021-10-22	3.5	CVE-2020-36493 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dedecms -- dedecms	DedeCMS v7.5 SP2 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities in the component select_media.php via the `activepath`, `keyword`, `tag`, `fmdo=x&filename`, `CKEditor` and `CKEditorFuncNum` parameters.	2021-10-22	3.5	CVE-2020-36492 MISC
dedecms -- dedecms	DedeCMS v7.5 SP2 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities in the component tags_main.php via the `activepath`, `keyword`, `tag`, `fmdo=x&filename`, `CKEditor` and `CKEditorFuncNum` parameters.	2021-10-22	3.5	CVE-2020-36491 MISC
dotnetfoundation -- piranha_cms	In PiranhaCMS, versions 7.0.0 to 9.1.1 are vulnerable to stored XSS due to the page title improperly sanitized. By creating a page with a specially crafted page title, a low privileged user can trigger arbitrary JavaScript execution.	2021-10-25	3.5	CVE-2021-25977 CONFIRM MISC
draytek -- vigorap_1000c_firmware	Draytek VigorAP 1000C contains a stored cross-site scripting (XSS) vulnerability in the RADIUS Setting - RADIUS Server Configuration module. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the username input field.	2021-10-22	3.5	CVE-2020-28968 MISC
dropouts -- air_share	Dropouts Technologies LLP Air Share v1.2 was discovered to contain a cross-site scripting (XSS) vulnerability in the devicename parameter. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the devicename information.	2021-10-22	3.5	CVE-2020-36489 MISC
easy_media_download_project -- easy_media_download	The Easy Media Download WordPress plugin before 1.1.7 does not escape the text argument of its shortcode, which could allow users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks.	2021-10-25	3.5	CVE-2021-24699 MISC
emarketdesign -- request_a_quote	The Request a Quote WordPress plugin before 2.3.5 does not sanitise, validate or escape some of its settings in the admin dashboard, leading to authenticated Stored Cross-Site Scripting issues even when the unfiltered_html capability is disallowed.	2021-10-25	3.5	CVE-2021-24489 MISC
ethereum -- go_ethereum	Go Ethereum is the official Golang implementation of the Ethereum protocol. Prior to version 1.10.9, a vulnerable node is susceptible to crash when processing a maliciously crafted message from a peer. Version v1.10.9 contains patches to the vulnerability. There are no known workarounds aside from upgrading.	2021-10-26	3.5	CVE-2021-41173 MISC MISC CONFIRM MISC
file_explorer_project -- file_explorer	An issue in the authentication mechanism in Nong Ge File Explorer v1.4 unauthenticated allows to access sensitive data.	2021-10-22	2.1	CVE-2020-23058 MISC
fork-cms -- fork_cms	Fork CMS Content Management System v5.8.0 was discovered to contain a cross-site scripting (XSS) vulnerability in the `Displayname` field when using the `Add`, `Edit` or `Register' functions. This vulnerability allows attackers to execute arbitrary web scripts or HTML.	2021-10-22	3.5	CVE-2020-23049 MISC
froxlor -- froxlor	Multiple cross-site scripting (XSS) vulnerabilities in the Customer Add module of Foxlor v0.10.16 allows attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the name, firstname, or username input fields.	2021-10-22	3.5	CVE-2020-28957 MISC
galette -- galette	Galette is a membership management web application geared towards non profit organizations. In versions prior to 0.9.5, malicious javascript code can be stored to be displayed later on self subscription page. The self subscription feature can be disabled as a workaround (this is the default state). Malicious javascript code can be executed (not stored) on login and retrieve password pages. This issue is patched in version 0.9.5.	2021-10-25	3.5	CVE-2021-21319 CONFIRM MISC MISC MISC MISC
getgrav -- grav	grav is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	2021-10-27	3.5	CVE-2021-3904 CONFIRM MISC
google -- android	In asf extractor, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05489178; Issue ID: ALPS05489178.	2021-10-25	2.1	CVE-2021-0613 MISC
google -- android	In flv extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561369; Issue ID: ALPS05561369.	2021-10-25	2.1	CVE-2021-0615 MISC
google -- android	In flv extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561384; Issue ID: ALPS05561384.	2021-10-25	2.1	CVE-2021-0414 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In flv extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561379; Issue ID: ALPS05561379.	2021-10-25	2.1	CVE-2021-0413 MISC
google -- android	In flv extractor, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561366; Issue ID: ALPS05561366.	2021-10-25	2.1	CVE-2021-0412 MISC
google -- android	In flv extractor, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561362; Issue ID: ALPS05561362.	2021-10-25	2.1	CVE-2021-0411 MISC
google -- android	In ape extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561389; Issue ID: ALPS05561389.	2021-10-25	2.1	CVE-2021-0616 MISC
google -- android	In ape extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561391; Issue ID: ALPS05561391.	2021-10-25	2.1	CVE-2021-0617 MISC
google -- android	In flv extractor, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561360; Issue ID: ALPS05561360.	2021-10-25	2.1	CVE-2021-0410 MISC
google -- android	In flv extractor, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561359; Issue ID: ALPS05561359.	2021-10-25	2.1	CVE-2021-0409 MISC
google -- android	In ape extractor, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05561394; Issue ID: ALPS05561394.	2021-10-25	2.1	CVE-2021-0618 MISC
google -- android	In getAllSubInfoList of SubscriptionController.java, there is a possible way to retrieve a long term identifier without the correct permissions due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-10Android ID: A-183612370	2021-10-22	2.1	CVE-2021-0643 MISC
google -- android	In memzero_explicit of compiler-clang.h, there is a possible bypass of defense in depth due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-171418586References: Upstream kernel	2021-10-25	2.1	CVE-2021-0938 MISC
google -- android	In wifi driver, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure to a proximal attacker under certain build conditions with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05560246; Issue ID: ALPS05551383.	2021-10-25	3.3	CVE-2021-0632 MISC
google -- android	In set_default_passthru_cfg of passthru.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-186026549References: N/A	2021-10-25	2.1	CVE-2021-0939 MISC
google -- android	In asf extractor, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05495528; Issue ID: ALPS05495528.	2021-10-25	2.1	CVE-2021-0614 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In RevertActiveSessions of apexd.cpp, there is a possible way to share the wrong file due to an unintentional MediaStore downgrade. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-193932765	2021-10-22	1.9	CVE-2021-0702 MISC
great-quotes_project -- great-quotes	The Great Quotes WordPress plugin through 1.0.0 does not sanitise and escape the Quote and Author fields of its Quotes, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed.	2021-10-25	3.5	CVE-2021-24785 MISC
hcltech -- traveler_companion	"HCL Traveler Companion is vulnerable to an iOS weak cryptographic process vulnerability via the included MobileIron AppConnect SDK"	2021-10-25	2.1	CVE-2020-14264 MISC
huawei -- cloudengine_12800_firmware	There is a use-after-free (UAF) vulnerability in Huawei products. An attacker may craft specific packets to exploit this vulnerability. Successful exploitation may cause the service abnormal. Affected product versions include:CloudEngine 12800 V200R005C10SPC800,V200R019C00SPC800;CloudEngine 5800 V200R005C10SPC800,V200R019C00SPC800;CloudEngine 6800 V200R005C10SPC800,V200R005C20SPC800,V200R019C00SPC800;CloudEngine 7800 V200R005C10SPC800,V200R019C00SPC800.	2021-10-27	3.3	CVE-2021-37122 MISC
huawei -- harmonyos	A component of the HarmonyOS has a Improper Input Validation vulnerability. Local attackers may exploit this vulnerability to cause nearby process crash.	2021-10-28	2.1	CVE-2021-22453 MISC
huawei -- harmonyos	A component of the HarmonyOS has a Improper Input Validation vulnerability. Local attackers may exploit this vulnerability to read at any address.	2021-10-28	2.1	CVE-2021-22452 MISC
huawei -- pc_smart_full_scene	There is a path traversal vulnerability in Huawei PC product. Because the product does not filter path with special characters,attackers can construct a file path with special characters to exploit this vulnerability. Successful exploitation could allow the attacker to transport a file to certain path.Affected product versions include:PC Smart Full Scene 11.1 versions PCManager 11.1.1.97.	2021-10-27	3.3	CVE-2021-37124 MISC
ibm -- engineering_lifecycle_optimization	IBM Jazz Team Server products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 199482.	2021-10-27	3.5	CVE-2021-29673 XF CONFIRM
ibm -- engineering_lifecycle_optimization	IBM Jazz Team Server products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2021-10-27	3.5	CVE-2021-29713 XF CONFIRM
lancom-systems -- lcos	ANCOM WLAN Controller (Wireless Series & Hotspot) WLC-1000 & WLC-4006 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities in the /authen/start/ module via the userid and password parameters.	2021-10-22	3.5	CVE-2020-23055 MISC
macrob7_macs_framework_content_management_system_project -- macrob7_macs_framework_content_management_system	Macrob7 Macs Framework Content Management System - 1.14f contains a cross-site scripting (XSS) vulnerability in the account reset function, which allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the e-mail input field.	2021-10-22	3.5	CVE-2020-36498 MISC
mara_cms_project -- mara_cms	A cross site scripting (XSS) vulnerability in menuedit.php of Mara CMS 7.5 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	2021-10-28	3.5	CVE-2020-25422 MISC
mcafee -- epolicy_orchestrator	Stored Cross-Site Scripting vulnerability in McAfee ePolicy Orchestrator (ePO) prior to 5.10 Update 11 allows ePO administrators to inject arbitrary web script or HTML via multiple parameters where the administrator's entries were not correctly sanitized.	2021-10-22	3.5	CVE-2021-31834 CONFIRM
motopress -- motopress-slider-lite	The Responsive WordPress Slider WordPress plugin through 2.2.0 does not sanitise and escape some of the Slider options, allowing Cross-Site Scripting payloads to be set in them. Furthermore, as by default any authenticated user is allowed to create Sliders (https://wordpress.org/support/topic/slider-can-be-changed-from-any-user-even-subscriber/, such settings can be changed in the plugin's settings), this would allow user with a role as low as subscriber to perform Cross-Site Scripting attacks against logged in admins viewing the slider list and could lead to privilege escalation by creating a rogue admin account for example.	2021-10-25	3.5	CVE-2021-24544 MISC
mybb -- mybb	MyBB before 1.8.28 allows stored XSS because the displayed Template Name value in the Admin CP's theme management is not escaped properly.	2021-10-26	3.5	CVE-2021-41866 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
newsoftwares -- folder_lock	Folder Lock v3.4.5 was discovered to contain a stored cross-site scripting (XSS) vulnerability in the Create Folder function under the 'create' module. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload as a path or folder name.	2021-10-22	3.5	CVE-2020-23039 MISC
nextcloud -- contacts	Nextcloud is an open-source, self-hosted productivity platform. The Nextcloud Contacts application prior to version 4.0.3 was vulnerable to a stored Cross-Site Scripting (XSS) vulnerability. For exploitation, a user would need to right-click on a malicious file and open the file in a new tab. Due the strict Content-Security-Policy shipped with Nextcloud, this issue is not exploitable on modern browsers supporting Content-Security-Policy. It is recommended that the Nextcloud Contacts application is upgraded to 4.0.3. As a workaround, one may use a browser that has support for Content-Security-Policy.	2021-10-25	3.5	CVE-2021-39221 CONFIRM MISC
nextcloud -- mail	Nextcloud is an open-source, self-hosted productivity platform The Nextcloud Mail application prior to versions 1.10.4 and 1.11.0 does by default not render images in emails to not leak the read state or user IP. The privacy filter failed to filter images with a relative protocol. It is recommended that the Nextcloud Mail application is upgraded to 1.10.4 or 1.11.0. There are no known workarounds aside from upgrading.	2021-10-25	3.5	CVE-2021-39220 MISC MISC CONFIRM
ninjaforms -- contact_form	The Ninja Forms Contact Form WordPress plugin before 3.5.8.2 does not sanitise and escape the custom class name of the form field created, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	2021-10-25	3.5	CVE-2021-24381 MISC
nvidia -- gpu_display_driver	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys), where a NULL pointer dereference in the kernel, created within user mode code, may lead to a denial of service in the form of a system crash.	2021-10-27	2.1	CVE-2021-1116 CONFIRM
nvidia -- gpu_display_driver	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for private IOCTLs, where an attacker with local unprivileged system access may cause a NULL pointer dereference, which may lead to denial of service in a component beyond the vulnerable component.	2021-10-27	2.1	CVE-2021-1115 CONFIRM
origincode -- smart-grid-gallery	The Video Gallery â€“ Vimeo and YouTube Gallery WordPress plugin through 1.1.4 does not escape the Title and Description of the videos in a gallery before outputting them in attributes, leading to Stored Cross-Site Scripting issues	2021-10-25	3.5	CVE-2021-24515 MISC
parallels -- parallels_desktop	This vulnerability allows local attackers to disclose sensitive information on affected installations of Parallels Desktop 16.1.3 (49160). An attacker must first obtain the ability to execute low-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the Toolgate component. The issue results from the lack of proper initialization of memory prior to accessing it. An attacker can leverage this in conjunction with other vulnerabilities to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-13592.	2021-10-25	2.1	CVE-2021-34855 N/A N/A
perfexcrm -- perfex_crm	Perfex CRM v2.4.4 was discovered to contain a stored cross-site scripting (XSS) vulnerability in the component ./clients/client via the company name parameter.	2021-10-22	3.5	CVE-2020-28961 MISC
pi-hole -- web_interface	Pi-hole's Web interface (based on AdminLTE) provides a central location to manage one's Pi-hole and review the statistics generated by FTLDNS. Prior to version 5.8, cross-site scripting is possible when adding a client via the groups-clients management page. This issue was patched in version 5.8.	2021-10-26	3.5	CVE-2021-41175 CONFIRM MISC MISC
shopware -- shopware	Shopware is open source e-commerce software. Versions prior to 5.7.6 contain a cross-site scripting vulnerability. This issue is patched in version 5.7.6. Two workarounds are available. Using the security plugin or adding a particular following config to the `.htaccess` file will protect against cross-site scripting in this case. There is also a config for those using nginx as a server. The plugin and the configs can be found on the GitHub Security Advisory page for this vulnerability.	2021-10-26	3.5	CVE-2021-41188 MISC MISC CONFIRM MISC MISC
sixapart -- movable_type	Cross-site scripting vulnerability in Movable Type Movable Type Premium 1.37 and earlier and Movable Type Premium Advanced 1.37 and earlier allows a remote authenticated attacker to inject an arbitrary script via unspecified vectors.	2021-10-26	3.5	CVE-2020-5669 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
strategy11 -- formidable_form_builder	The Formidable Form Builder â€“ Contact Form, Survey & Quiz Forms Plugin for WordPress plugin before 5.0.07 does not sanitise and escape its Form's Labels, allowing high privileged users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	2021-10-25	3.5	CVE-2021-24608 CONFIRM MISC
sugarcrm -- sugarcrm	Multiple cross-site scripting (XSS) vulnerabilities in the Support module of SugarCRM v6.5.18 allows attackers to execute arbitrary web scripts or HTML via crafted payloads entered into the primary address state or alternate address state input fields.	2021-10-22	3.5	CVE-2020-36501 MISC
sugarcrm -- sugarcrm	SugarCRM v6.5.18 was discovered to contain a cross-site scripting (XSS) vulnerability in the Create Employee module. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the First Name or Last Name input fields.	2021-10-22	3.5	CVE-2020-28955 MISC
sugarcrm -- sugarcrm	Multiple cross-site scripting (XSS) vulnerabilities in the Sales module of SugarCRM v6.5.18 allows attackers to execute arbitrary web scripts or HTML via crafted payloads entered into the primary address state or alternate address state input fields.	2021-10-22	3.5	CVE-2020-28956 MISC
taotesting -- assessment_platform	TAO Open Source Assessment Platform v3.3.0 RC02 was discovered to contain a cross-site scripting (XSS) vulnerability in the content parameter of the Rubric Block (Add) module. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the rubric name value.	2021-10-22	3.5	CVE-2020-36499 MISC
tibco -- nimbus	The Web Reporting component of TIBCO Software Inc.'s TIBCO Nimbus contains easily exploitable Stored Cross Site Scripting (XSS) vulnerabilities that allow a low privileged attacker to social engineer a legitimate user with network access to execute scripts targeting the affected system or the victim's local system. A successful attack using this vulnerability requires human interaction from a person other than the attacker. Affected releases are TIBCO Software Inc.'s TIBCO Nimbus: versions 10.4.0 and below.	2021-10-26	3.5	CVE-2021-35499 CONFIRM CONFIRM
vfbpro -- visual_form_builder	The Visual Form Builder WordPress plugin before 3.0.4 does not sanitise or escape its Form Name, allowing high privilege users such as admin to set Cross-Site Scripting payload in them, even when the unfiltered_html capability is disallowed	2021-10-25	3.5	CVE-2021-24514 MISC
video_player_for_youtube_project -- video_player_for_youtube	The Video Player for YouTube WordPress plugin before 1.4 does not sanitise or validate the parameters from its shortcode, allowing users with a role as low as contributor to set Cross-Site Scripting payload in them which will be triggered in the page/s with the embed malicious shortcode	2021-10-25	3.5	CVE-2021-24414 MISC
wp-special-textboxes_project -- wp-special-textboxes	The Special Text Boxes WordPress plugin through 5.9.109 does not sanitise or escape some of its settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed.	2021-10-25	3.5	CVE-2021-24485 MISC

Back to top

Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
abb -- pcm600	A certificate validation vulnerability in PCM600 Update Manager allows attacker to get unwanted software packages to be installed on computer which has PCM600 installed.	2021-10-28	not yet calculated	CVE-2021-22278 MISC MISC
apple -- ios_and_ipados	The issue was addressed with improved permissions logic. This issue is fixed in iOS 15 and iPadOS 15. An attacker with physical access to a device may be able to see private contact information.	2021-10-28	not yet calculated	CVE-2021-30816 MISC
apple -- macos	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Monterey 12.0.1, Security Update 2021-007 Catalina, macOS Big Sur 11.6.1. A malicious application may be able to execute arbitrary code with kernel privileges.	2021-10-28	not yet calculated	CVE-2021-30824 MISC MISC MISC
apple -- macos	A resource exhaustion issue was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1. An attacker in a privileged network position may be able to perform denial of service.	2021-10-28	not yet calculated	CVE-2020-10005 MISC
apple -- macos	This issue was addressed with improved checks. This issue is fixed in macOS Monterey 12.0.1. A person with access to a host Mac may be able to bypass the Login Window in Remote Desktop for a locked instance of macOS.	2021-10-28	not yet calculated	CVE-2021-30813 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- macos	A permissions issue was addressed with improved validation. This issue is fixed in macOS Big Sur 11.5. A malicious application may be able to access data about the accounts the user is using Family Sharing with.	2021-10-28	not yet calculated	CVE-2021-30817 MISC
apple -- macos	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.0.1, Security Update 2021-007 Catalina, macOS Big Sur 11.6.1. A malicious application may be able to execute arbitrary code with kernel privileges.	2021-10-28	not yet calculated	CVE-2021-30821 MISC MISC MISC
apple -- macos	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1. A malicious application may be able to read restricted memory.	2021-10-28	not yet calculated	CVE-2020-29629 MISC
apple -- macos	This issue was addressed with improved checks. This issue is fixed in macOS Monterey 12.0.1. Unpacking a maliciously crafted archive may allow an attacker to write arbitrary files.	2021-10-28	not yet calculated	CVE-2021-30833 MISC
apple -- multiple_products	A type confusion issue was addressed with improved state handling. This issue is fixed in iOS 14.8 and iPadOS 14.8, tvOS 15, iOS 15 and iPadOS 15, Safari 15, watchOS 8. Processing maliciously crafted web content may lead to arbitrary code execution.	2021-10-28	not yet calculated	CVE-2021-30818 MISC MISC MISC MISC MISC
apple -- multiple_products	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Monterey 12.0.1, iOS 14.8 and iPadOS 14.8, tvOS 15, Safari 15, watchOS 8. An attacker in a privileged network position may be able to bypass HSTS.	2021-10-28	not yet calculated	CVE-2021-30823 MISC MISC MISC MISC MISC
apple -- multiple_products	This issue was addressed with improved checks. This issue is fixed in tvOS 15, watchOS 8, iOS 15 and iPadOS 15. A malicious application may be able to modify protected parts of the file system.	2021-10-28	not yet calculated	CVE-2021-30808 MISC MISC MISC
apple -- multiple_products	A use after free issue was addressed with improved memory management. This issue is fixed in Safari 15, tvOS 15, watchOS 8, iOS 15 and iPadOS 15. Processing maliciously crafted web content may lead to arbitrary code execution.	2021-10-28	not yet calculated	CVE-2021-30809 MISC MISC MISC MISC
apple -- multiple_products	A memory corruption issue was addressed with improved input validation. This issue is fixed in tvOS 15, watchOS 8, iOS 15 and iPadOS 15. Processing a maliciously crafted image may lead to arbitrary code execution.	2021-10-28	not yet calculated	CVE-2021-30814 MISC MISC MISC
apple -- multiple_products	A logic issue was addressed with improved state management. This issue is fixed in watchOS 7.6, macOS Big Sur 11.5. Visiting a maliciously crafted webpage may lead to a system denial of service.	2021-10-28	not yet calculated	CVE-2021-1821 MISC MISC
apple -- multiple_products	An out-of-bounds write was addressed with improved input validation. This issue is fixed in iOS 14.2 and iPadOS 14.2, macOS Big Sur 11.0.1. Processing a maliciously crafted PDF may lead to arbitrary code execution.	2021-10-28	not yet calculated	CVE-2020-9897 MISC MISC
apple -- multiple_products	An out-of-bounds read was addressed with improved input validation. This issue is fixed in tvOS 15, watchOS 8, iOS 15 and iPadOS 15. Processing a maliciously crafted font may result in the disclosure of process memory.	2021-10-28	not yet calculated	CVE-2021-30831 MISC MISC MISC
apple -- multiple_products	A logic issue was addressed with improved state management. This issue is fixed in iOS 14.8 and iPadOS 14.8, tvOS 15, iOS 15 and iPadOS 15, watchOS 8, Security Update 2021-007 Catalina. Processing a malicious audio file may result in unexpected application termination or arbitrary code execution.	2021-10-28	not yet calculated	CVE-2021-30834 MISC MISC MISC MISC MISC
apple -- multiple_products	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 14.8 and iPadOS 14.8, tvOS 15, watchOS 8, iOS 15 and iPadOS 15. Processing a maliciously crafted audio file may disclose restricted memory.	2021-10-28	not yet calculated	CVE-2021-30836 MISC MISC MISC MISC
apple -- multiple_products	This issue was addressed with improved checks. This issue is fixed in tvOS 15, watchOS 8, iOS 15 and iPadOS 15. Processing a maliciously crafted dfont file may lead to arbitrary code execution.	2021-10-28	not yet calculated	CVE-2021-30840 MISC MISC MISC
baijiacms -- baijiacms	A directory traversal vulnerability in the component system/manager/class/web/database.php was discovered in Baijiacms V4 which allows attackers to arbitrarily delete folders on the server via the "id" parameter.	2021-10-29	not yet calculated	CVE-2020-25873 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bind -- bind	In BIND 9.3.0 -> 9.11.35, 9.12.0 -> 9.16.21, and versions 9.9.3-S1 -> 9.11.35-S1 and 9.16.8-S1 -> 9.16.21-S1 of BIND Supported Preview Edition, as well as release versions 9.17.0 -> 9.17.18 of the BIND 9.17 development branch, exploitation of broken authoritative servers using a flaw in response processing can cause degradation in BIND resolver performance. The way the lame cache is currently designed makes it possible for its internal data structures to grow almost infinitely, which may cause significant delays in client query processing.	2021-10-27	not yet calculated	CVE-2021-25219 CONFIRM DEBIAN
bitdefender -- endpoint_secruity_tools	Execution with Unnecessary Privileges vulnerability in Bitdefender Endpoint Security Tools, Total Security allows a local attacker to elevate to 'NT AUTHORITY\System. Impersonation enables the server thread to perform actions on behalf of the client but within the limits of the client's security context. This issue affects: Bitdefender Endpoint Security Tools versions prior to 7.2.1.65. Bitdefender Total Security versions prior to 25.0.26.	2021-10-28	not yet calculated	CVE-2021-3576 MISC
bitdefender -- endpoint_secruity_tools	Incorrect Default Permissions vulnerability in the bdservicehost.exe and Vulnerability.Scan.exe components as used in Bitdefender Endpoint Security Tools for Windows, Total Security allows a local attacker to elevate privileges to NT AUTHORITY\SYSTEM This issue affects: Bitdefender Endpoint Security Tools for Windows versions prior to 7.2.1.65. Bitdefender Total Security versions prior to 7.2.1.65.	2021-10-28	not yet calculated	CVE-2021-3579 MISC
bitdefender -- gravityzone	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in the UpdateServer component of Bitdefender GravityZone allows an attacker to execute arbitrary code on vulnerable instances. This issue affects: Bitdefender GravityZone versions prior to 3.3.8.249.	2021-10-28	not yet calculated	CVE-2021-3823 CONFIRM
bookstack -- bookstack	bookstack is vulnerable to Unrestricted Upload of File with Dangerous Type	2021-10-27	not yet calculated	CVE-2021-3906 MISC CONFIRM
calibre -- calibre	A untrusted search path issue was found in Calibre at devices/linux_mount_helper.c leading to the ability of unprivileged users to execute any program as root.	2021-10-27	not yet calculated	CVE-2011-4125 MISC MISC MISC MISC
calibre -- calibre	Race condition issues were found in Calibre at devices/linux_mount_helper.c allowing unprivileged users the ability to mount any device to anywhere.	2021-10-27	not yet calculated	CVE-2011-4126 MISC MISC MISC MISC
calibre -- calibre	Input validation issues were found in Calibre at devices/linux_mount_helper.c which can lead to argument injection and elevation of privileges.	2021-10-27	not yet calculated	CVE-2011-4124 MISC MISC MISC MISC
cfeengine -- enterprise	CFEngine Enterprise 3.15.0 through 3.15.4 has Missing SSL Certificate Validation.	2021-10-27	not yet calculated	CVE-2021-36756 MISC MISC
cfeengine -- enterprise	The Hub in CFEngine Enterprise 3.6.7 through 3.18.0 has Insecure Permissions that allow local Information Disclosure.	2021-10-27	not yet calculated	CVE-2021-38379 MISC MISC
dext5 -- dext5	DEXT5 Upload 5.0.0.117 and earlier versions contain a vulnerability, which could allow remote attacker to download and execute remote file by setting the argument, variable in the activeX module. This can be leveraged for code execution.	2021-10-28	not yet calculated	CVE-2020-7875 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dhis2 -- dhis2	DHIS 2 is an information system for data capture, management, validation, analytics and visualization. A SQL Injection vulnerability in the Tracker component in DHIS2 Server allows authenticated remote attackers to execute arbitrary SQL commands via unspecified vectors. This vulnerability affects the `/api/trackedEntityInstances` and `/api/trackedEntityInstances/query` API endpoints in all DHIS2 versions 2.34, 2.35, and 2.36. It also affects versions 2.32 and 2.33 which have reached _end of support_ - exceptional security updates have been added to the latest *end of support* builds for these versions. Versions 2.31 and older are unaffected. The system is vulnerable to attack only from users that are logged in to DHIS2, and there is no known way of exploiting the vulnerability without first being logged in as a DHIS2 user. The vulnerability is not exposed to a non-malicious user - the vulnerability requires a conscious attack to be exploited. A successful exploit of this vulnerability could allow the malicious user to read, edit and delete data in the DHIS2 instance. There are no known exploits of the security vulnerabilities addressed by these patch releases. Security patches are available in DHIS2 versions 2.32-EOS, 2.33-EOS, 2.34.7, 2.35.7, and 2.36.4. There is no straightforward known workaround for DHIS2 instances using the Tracker functionality other than upgrading the affected DHIS2 server to one of the patches in which this vulnerability has been fixed. For implementations which do NOT use Tracker functionality, it may be possible to block all network access to POST to the `/api/trackedEntityInstances`, and `/api/trackedEntityInstances/query` endpoints as a temporary workaround while waiting to upgrade.	2021-10-29	not yet calculated	CVE-2021-39179 CONFIRM MISC MISC
dspace -- dspace	DSpace is an open source turnkey repository application. In version 7.0, any community or collection administrator can escalate their permission up to become system administrator. This vulnerability only exists in 7.0 and does not impact 6.x or below. This issue is patched in version 7.1. As a workaround, users of 7.0 may temporarily disable the ability for community or collection administrators to manage permissions or workflows settings.	2021-10-29	not yet calculated	CVE-2021-41189 MISC MISC CONFIRM MISC
dxgkddiescape -- dxgkddiescape	Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, where an attacker through specific configuration and with local unprivileged system access may cause improper input validation, which may lead to denial of service.	2021-10-27	not yet calculated	CVE-2021-1117 CONFIRM
firefly-iii -- firefly-iii	firefly-iii is vulnerable to Cross-Site Request Forgery (CSRF)	2021-10-27	not yet calculated	CVE-2021-3901 MISC CONFIRM
flatcore-cms -- flatcore-cms	flatcore-cms is vulnerable to Unrestricted Upload of File with Dangerous Type	2021-10-28	not yet calculated	CVE-2021-3745 CONFIRM MISC
fluentd -- fluentd	Fluentd collects events from various data sources and writes them to files to help unify logging infrastructure. The parser_apache2 plugin in Fluentd v0.14.14 to v1.14.1 suffers from a regular expression denial of service (ReDoS) vulnerability. A broken apache log with a certain pattern of string can spend too much time in a regular expression, resulting in the potential for a DoS attack. This issue is patched in version 1.14.2 There are two workarounds available. Either don't use parser_apache2 for parsing logs (which cannot guarantee generated by Apache), or put patched version of parser_apache2.rb into /etc/fluent/plugin directory (or any other directories specified by the environment variable `FLUENT_PLUGIN` or `--plugin` option of fluentd).	2021-10-29	not yet calculated	CVE-2021-41186 MISC MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
freeswitch -- freeswitch	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to version 1.10.7, FreeSWITCH does not authenticate SIP MESSAGE requests, leading to spam and message spoofing. By default, SIP requests of the type MESSAGE (RFC 3428) are not authenticated in the affected versions of FreeSWITCH. MESSAGE requests are relayed to SIP user agents registered with the FreeSWITCH server without requiring any authentication. Although this behaviour can be changed by setting the `auth-messages` parameter to `true`, it is not the default setting. Abuse of this security issue allows attackers to send SIP MESSAGE messages to any SIP user agent that is registered with the server without requiring authentication. Additionally, since no authentication is required, chat messages can be spoofed to appear to come from trusted entities. Therefore, abuse can lead to spam and enable social engineering, phishing and similar attacks. This issue is patched in version 1.10.7. Maintainers recommend that this SIP message type is authenticated by default so that FreeSWITCH administrators do not need to be explicitly set the `auth-messages` parameter. When following such a recommendation, a new parameter can be introduced to explicitly disable authentication.	2021-10-25	not yet calculated	CVE-2021-37624 CONFIRM MISC MLIST FULLDISC MISC
frogcms -- frogcms	A vulnerability exists within the FileManagerController.php function in FrogCMS 0.9.5 which allows an attacker to perform a directory traversal attack via a GET request urlencode parameter.	2021-10-29	not yet calculated	CVE-2020-25872 MISC
godomall5 -- godomall5	The move_uploaded_file function in godomall5 does not perform an integrity check of extension or authority when user upload file. This vulnerability allows an attacker to execute an remote arbitrary code.	2021-10-27	not yet calculated	CVE-2021-26610 MISC
gradle -- enterprise	In Gradle Enterprise before 2021.3 (and Enterprise Build Cache Node before 10.0), there is potential cache poisoning and remote code execution when running the build cache node with its default configuration. This configuration allows anonymous access to the configuration user interface and anonymous write access to the build cache. If access control to the build cache is not changed from the default open configuration, a malicious actor with network access can populate the cache with manipulated entries that may execute malicious code as part of a build process. This applies to the build cache provided with Gradle Enterprise and the separate build cache node service if used. If access control to the user interface is not changed from the default open configuration, a malicious actor can undo build cache access control in order to populate the cache with manipulated entries that may execute malicious code as part of a build process. This does not apply to the build cache provided with Gradle Enterprise, but does apply to the separate build cache node service if used.	2021-10-27	not yet calculated	CVE-2021-41589 MISC MISC
gradle -- enterprise	In Gradle Enterprise through 2021.3, probing of the server-side network environment can occur via an SMTP configuration test. The installation configuration user interface available to administrators allows testing the configured SMTP server settings. This test function can be used to identify the listening TCP ports available to the server, revealing information about the internal network environment.	2021-10-27	not yet calculated	CVE-2021-41590 MISC MISC
gradle -- enterprise	An issue was discovered in Gradle Enterprise before 2021.1.2. There is potential remote code execution via the application startup configuration. The installation configuration user interface (available to administrators) allows specifying arbitrary Java Virtual Machine startup options. Some of these options, such as -XX:OnOutOfMemoryError, allow specifying a command to be run on the host. This can be abused to run arbitrary commands on the host, should an attacker gain administrative access to the application.	2021-10-27	not yet calculated	CVE-2021-41619 MISC MISC
grandstream -- ht801_analog_telephone_adaptor	An issue was discovered on the Grandstream HT801 Analog Telephone Adaptor before 1.0.29.8. From the limited configuration shell, it is possible to set the malicious gdb_debug_server variable. As a result, after a reboot, the device downloads and executes malicious scripts from an attacker-defined host.	2021-10-28	not yet calculated	CVE-2021-37915 MISC MISC MISC
grandstream -- ht801_devices	Multiple buffer overflows in the limited configuration shell (/sbin/gs_config) on Grandstream HT801 devices before 1.0.29 allow remote authenticated users to execute arbitrary code as root via a crafted manage_if setting, thus bypassing the intended restrictions of this shell and taking full control of the device. There are default weak credentials that can be used to authenticate.	2021-10-28	not yet calculated	CVE-2021-37748 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
harmonyos -- harmonyos	A component of the HarmonyOS has a NULL Pointer Dereference vulnerability. Local attackers may exploit this vulnerability to cause System functions which are unavailable.	2021-10-28	not yet calculated	CVE-2021-22459 MISC
harmonyos -- harmonyos	A component of the HarmonyOS has a Insufficient Verification of Data Authenticity vulnerability. Local attackers may exploit this vulnerability to bypass the control mechanism.	2021-10-28	not yet calculated	CVE-2021-22460 MISC
harmonyos -- harmonyos	A component of the HarmonyOS has a Incomplete Cleanup vulnerability. Local attackers may exploit this vulnerability to cause memory exhaustion.	2021-10-28	not yet calculated	CVE-2021-22450 MISC
harmonyos -- harmonyos	A component of the HarmonyOS has a Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability. Local attackers may exploit this vulnerability to cause arbitrary code execution.	2021-10-28	not yet calculated	CVE-2021-22458 MISC
harmonyos -- harmonyos	A component of the HarmonyOS has a Improper Input Validation vulnerability. Local attackers may exploit this vulnerability to cause out-of-bounds write.	2021-10-28	not yet calculated	CVE-2021-22457 MISC
harmonyos -- harmonyos	A component of the HarmonyOS has a Data Processing Errors vulnerability. Local attackers may exploit this vulnerability to cause Kernel System unavailable.	2021-10-28	not yet calculated	CVE-2021-22456 MISC
harmonyos -- harmonyos	A component of the HarmonyOS has a Integer Overflow or Wraparound vulnerability. Local attackers may exploit this vulnerability to cause the memory which is not released.	2021-10-28	not yet calculated	CVE-2021-22455 MISC
harmonyos -- harmonyos	A component of the HarmonyOS has a External Control of System or Configuration Setting vulnerability. Local attackers may exploit this vulnerability to cause core dump.	2021-10-28	not yet calculated	CVE-2021-22454 MISC
harmonyos -- harmonyos	A component of the HarmonyOS has a Integer Overflow or Wraparound vulnerability. Local attackers may exploit this vulnerability to cause memory overwriting.	2021-10-28	not yet calculated	CVE-2021-22451 MISC
harmonyos -- harmonyos	A component of the HarmonyOS has a NULL Pointer Dereference vulnerability. Local attackers may exploit this vulnerability to cause kernel crash.	2021-10-28	not yet calculated	CVE-2021-22462 MISC
harmonyos -- harmonyos	A component of the HarmonyOS has a Use After Free vulnerability . Local attackers may exploit this vulnerability to cause Kernel Information disclosure.	2021-10-28	not yet calculated	CVE-2021-22463 MISC
harmonyos -- harmonyos	A component of the HarmonyOS has a NULL Pointer Dereference vulnerability. Local attackers may exploit this vulnerability to cause nearby process crash.	2021-10-28	not yet calculated	CVE-2021-22471 MISC
harmonyos -- harmonyos	A component of the HarmonyOS has a Privileges Controls vulnerability. Local attackers may exploit this vulnerability to expand the Recording Trusted Domain.	2021-10-28	not yet calculated	CVE-2021-22470 MISC
harmonyos -- harmonyos	A component of the HarmonyOS has a Out-of-bounds Read vulnerability. Local attackers may exploit this vulnerability to cause kernel out-of-bounds read.	2021-10-28	not yet calculated	CVE-2021-22469 MISC
harmonyos -- harmonyos	A component of the HarmonyOS has a Exposure of Sensitive Information to an Unauthorized Actor vulnerability. Local attackers may exploit this vulnerability to cause kernel address leakage.	2021-10-28	not yet calculated	CVE-2021-22468 MISC
harmonyos -- harmonyos	A component of the HarmonyOS has a Improper Input Validation vulnerability. Local attackers may exploit this vulnerability to read at any address.	2021-10-28	not yet calculated	CVE-2021-22467 MISC
harmonyos -- harmonyos	A component of the HarmonyOS has a Use After Free vulnerability. Local attackers may exploit this vulnerability to cause kernel crash.	2021-10-28	not yet calculated	CVE-2021-22466 MISC
harmonyos -- harmonyos	A component of the HarmonyOS has a Heap-based Buffer Overflow vulnerability. Local attackers may exploit this vulnerability to cause Kernel System unavailable.	2021-10-28	not yet calculated	CVE-2021-22465 MISC
harmonyos -- harmonyos	A component of the HarmonyOS has a Out-of-bounds Read vulnerability. Local attackers may exploit this vulnerability to cause system Soft Restart.	2021-10-28	not yet calculated	CVE-2021-22464 MISC
harmonyos -- harmonyos	A component of the HarmonyOS has a Allocation of Resources Without Limits or Throttling vulnerability. Local attackers may exploit this vulnerability to cause nearby process crash.	2021-10-28	not yet calculated	CVE-2021-22461 MISC
hewlett_packard -- laserjet	Certain HP Enterprise LaserJet and PageWide MFPs may be vulnerable to stored cross site scripting (XSS).	2021-10-29	not yet calculated	CVE-2021-3662 MISC
hewlett_packard -- officejet_7110_eprinter	A potential security vulnerability has been identified for the HP OfficeJet 7110 Wide Format ePrinter that enables Cross-Site Scripting (XSS).	2021-10-29	not yet calculated	CVE-2021-3441 MISC
huawei -- multiple_devices	There is a SSID vulnerability with Wi-Fi network connections in Huawei devices.Successful exploitation of this vulnerability may affect service confidentiality.	2021-10-28	not yet calculated	CVE-2021-22485 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
huawei -- smartphones	There is an Improper verification vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service confidentiality.	2021-10-28	not yet calculated	CVE-2021-22472 MISC
huawei -- smartphones	There is an Uncaught Exception vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability will cause the app to exit unexpectedly.	2021-10-28	not yet calculated	CVE-2021-22406 MISC
huawei -- smartphones	There is an Out-of-bounds read vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may affect service availability.	2021-10-28	not yet calculated	CVE-2021-22487 MISC
huawei -- smartphones	There is a issue that trustlist strings being repeatedly inserted into the linked list in Huawei Smartphone due to race conditions. Successful exploitation of this vulnerability can cause exceptions when managing the system trustlist.	2021-10-28	not yet calculated	CVE-2021-36994 MISC
huawei -- smartphones	There is a issue that nodes in the linked list being freed for multiple times in Huawei Smartphone due to race conditions. Successful exploitation of this vulnerability can cause the system to restart.	2021-10-28	not yet calculated	CVE-2021-36987 MISC
huawei -- smartphones	There is an Unauthorized file access vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability by modifying soft links may tamper with the files restored from backups.	2021-10-28	not yet calculated	CVE-2021-36995 MISC
huawei -- smartphones	There is a Public key verification vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service confidentiality.	2021-10-28	not yet calculated	CVE-2021-36992 MISC
huawei -- smartphones	There is a issue of Unstandardized field names in Huawei Smartphone. Successful exploitation of this vulnerability may affect service confidentiality.	2021-10-28	not yet calculated	CVE-2021-22486 MISC
huawei -- smartphones	There is a Permission verification vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect the device performance.	2021-10-28	not yet calculated	CVE-2021-22490 MISC
huawei -- smartphones	There is a Low memory error in Huawei Smartphone due to the unlimited size of images to be parsed.Successful exploitation of this vulnerability may cause the Gallery or Files app to exit unexpectedly.	2021-10-28	not yet calculated	CVE-2021-36997 MISC
huawei -- smartphones	There is a Logic Bypass vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service integrity and availability.	2021-10-28	not yet calculated	CVE-2021-22436 MISC
huawei -- smartphones	There is an Improper permission management vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service confidentiality.	2021-10-28	not yet calculated	CVE-2021-22475 MISC
huawei -- smartphones	There is an Out-of-bounds memory access in Huawei Smartphone.Successful exploitation of this vulnerability may cause process exceptions.	2021-10-28	not yet calculated	CVE-2021-22474 MISC
huawei -- smartphones	There is a vulnerability of hijacking unverified providers in Huawei Smartphone.Successful exploitation of this vulnerability may allow attackers to hijack the device and forge UIs to induce users to execute malicious commands.	2021-10-28	not yet calculated	CVE-2021-22403 MISC
huawei -- smartphones	There is a Memory out-of-bounds access vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause malicious code to be executed.	2021-10-28	not yet calculated	CVE-2021-37002 MISC
huawei -- smartphones	There is an Improper verification vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause transmission of certain virtual information.	2021-10-28	not yet calculated	CVE-2021-36996 MISC
huawei -- smartphones	There is a Register tampering vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may allow the register value to be modified.	2021-10-28	not yet calculated	CVE-2021-37001 MISC
huawei -- smartphones	There is an Improper verification vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may allow attempts to read an array that is out of bounds.	2021-10-28	not yet calculated	CVE-2021-36998 MISC
huawei -- smartphones	There is a Buffer overflow vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability by sending malicious images and inducing users to open the images may cause remote code execution.	2021-10-28	not yet calculated	CVE-2021-36999 MISC
huawei -- smartphones	There is a Memory leaks vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service availability.	2021-10-28	not yet calculated	CVE-2021-36993 MISC
huawei -- smartphones	There is a Parameter verification issue in Huawei Smartphone.Successful exploitation of this vulnerability can affect service integrity.	2021-10-28	not yet calculated	CVE-2021-36988 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
huawei -- smartphones	There is a Kernel crash vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may escalate permissions.	2021-10-28	not yet calculated	CVE-2021-36989 MISC
huawei -- smartphones	There is a vulnerability of tampering with the kernel in Huawei Smartphone.Successful exploitation of this vulnerability may escalate permissions.	2021-10-28	not yet calculated	CVE-2021-36990 MISC
huawei -- smartphones	There is an Unauthorized file access vulnerability in Huawei Smartphone due to unstandardized path input.Successful exploitation of this vulnerability by creating malicious file paths can cause unauthorized file access.	2021-10-28	not yet calculated	CVE-2021-36991 MISC
huawei -- smartphones	There is a vulnerability of tampering with the kernel in Huawei Smartphone.Successful exploitation of this vulnerability may escalate permissions.	2021-10-28	not yet calculated	CVE-2021-36986 MISC
huawei -- smartphones	There is an Input verification vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service availability.	2021-10-28	not yet calculated	CVE-2021-22491 MISC
huawei -- smartphones	There is an Unauthorized file access vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability by modifying soft links may tamper with the files restored from backups.	2021-10-28	not yet calculated	CVE-2021-22488 MISC
huawei -- smartphones	There is a issue of IP address spoofing in Huawei Smartphone. Successful exploitation of this vulnerability may cause DoS.	2021-10-28	not yet calculated	CVE-2021-22483 MISC
huawei -- smartphones	There is an Uninitialized variable vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause transmission of invalid data.	2021-10-28	not yet calculated	CVE-2021-22482 MISC
huawei -- smartphones	There is a Verification errors vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service confidentiality.	2021-10-28	not yet calculated	CVE-2021-22481 MISC
huawei -- smartphones	There is an Authentication vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service confidentiality.	2021-10-28	not yet calculated	CVE-2021-22473 MISC
huawei -- smartphones	There is a Configuration defects in Huawei Smartphone.Successful exploitation of this vulnerability may affect service confidentiality.	2021-10-28	not yet calculated	CVE-2021-22407 MISC
huawei -- smartphones	There is a Code injection vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may exhaust system resources and cause the system to restart.	2021-10-28	not yet calculated	CVE-2021-36985 MISC
hznuoj -- hznuoj	A cross-site scripting (XSS) vulnerability was discovered in the OJ/admin-tool /cal_scores.php function of HZNUOJ v1.0.	2021-10-28	not yet calculated	CVE-2020-22312 MISC
ibm -- i2_ibase	IBM i2 iBase 8.9.13 and 9.0.0 could allow a local attacker to obtain sensitive information due to insufficient session expiration. IBM X-Force ID: 206213.	2021-10-27	not yet calculated	CVE-2021-29868 CONFIRM XF
ibm -- jazz_team_server	IBM Jazz Team Server products is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks.	2021-10-27	not yet calculated	CVE-2021-29844 XF CONFIRM
ibm -- jazz_team_server	IBM Jazz Team Server products stores user credentials in clear text which can be read by an authenticated user. IBM X-Force ID: 203172.	2021-10-27	not yet calculated	CVE-2021-29786 XF CONFIRM
installbuilder -- installbuilder	Under certain circumstances, when manipulating the Windows registry, InstallBuilder uses the reg.exe system command. The full path to the command is not enforced, which results in a search in the search path until a binary can be identified. This makes the installer/uninstaller vulnerable to Path Interception by Search Order Hijacking, potentially allowing an attacker to plant a malicious reg.exe command so it takes precedence over the system command. The vulnerability only affects Windows installers.	2021-10-29	not yet calculated	CVE-2021-22037 MISC
installbuilder -- installbuilder	On Windows, the uninstaller binary copies itself to a fixed temporary location, which is then executed (the originally called uninstaller exits, so it does not block the installation directory). This temporary location is not randomized and does not restrict access to Administrators only so a potential attacker could plant a binary to replace the copied binary right before it gets called, thus gaining Administrator privileges (if the original uninstaller was executed as Administrator). The vulnerability only affects Windows installers.	2021-10-29	not yet calculated	CVE-2021-22038 MISC
irfanview -- irfanview	IrfanView 4.54 allows attackers to cause a denial of service or possibly other unspecified impacts via a crafted .cr2 file, related to a "Data from Faulting Address controls Branch Selection starting at FORMATS!GetPlugInInfo+0x00000000000047f6".	2021-10-28	not yet calculated	CVE-2020-23549 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
irfanview -- irfanview	IrfanView 4.54 allows attackers to cause a denial of service or possibly other unspecified impacts via a crafted XBM file, related to a "Data from Faulting Address is used as one or more arguments in a subsequent Function Call starting at FORMATS!ReadMosaic+0x0000000000000981.	2021-10-28	not yet calculated	CVE-2020-23546 MISC MISC MISC
jupyterhub -- jupyterhub	FirstUseAuthenticator is a JupyterHub authenticator that helps new users set their password on their first login to JupyterHub. When JupyterHub is used with FirstUseAuthenticator, a vulnerability in versions prior to 1.0.0 allows unauthorized access to any user's account if `create_users=True` and the username is known or guessed. One may upgrade to version 1.0.0 or apply a patch manually to mitigate the vulnerability. For those who cannot upgrade, there is no complete workaround, but a partial mitigation exists. One can disable user creation with `c.FirstUseAuthenticator.create_users = False`, which will only allow login with fully normalized usernames for already existing users prior to jupyterhub-firstuserauthenticator 1.0.0. If any users have never logged in with their normalized username (i.e. lowercase), they will still be vulnerable until a patch or upgrade occurs.	2021-10-28	not yet calculated	CVE-2021-41194 MISC CONFIRM MISC
kiwi -- syslog_server	A missing HTTP header (X-Frame-Options) in Kiwi Syslog Server has left customers vulnerable to click jacking. Clickjacking is an attack that occurs when an attacker uses a transparent iframe in a window to trick a user into clicking on an actionable item, such as a button or link, to another server in which they have an identical webpage. The attacker essentially hijacks the user activity intended for the original server and sends them to the other server. This is an attack on both the user and the server.	2021-10-29	not yet calculated	CVE-2021-35237 MISC MISC
libmysofa -- libmysofa	libmysofa is vulnerable to Heap-based Buffer Overflow	2021-10-29	not yet calculated	CVE-2021-3756 MISC CONFIRM
linux -- linux_kernel	An issue was discovered in the Linux kernel before 5.14.8. A use-after-free in selinux_ptrace_traceme (aka the SELinux handler for PTRACE_TRACEME) could be used by local attackers to cause memory corruption and escalate privileges, aka CID-a3727a8bac0a. This occurs because of an attempt to access the subjective credentials of another task.	2021-10-28	not yet calculated	CVE-2021-43057 MISC MISC MISC
linux -- linux_kernel	An issue was discovered in the Linux kernel for powerpc before 5.14.15. It allows a malicious KVM guest to crash the host, when the host is running on Power8, due to an arch/powerpc/kvm/book3s_hv_rmhandlers.S implementation bug in the handling of the SRR1 register values.	2021-10-28	not yet calculated	CVE-2021-43056 MISC MISC MISC MLIST
m-files_web -- m-files_web	In M-Files Web product with versions before 20.10.9524.1 and 20.10.9445.0, a remote attacker could use a flaw to obtain unauthenticated access to 3rd party component license key information on server.	2021-10-28	not yet calculated	CVE-2021-37254 MISC MISC
mara -- mara	A remote code execution (RCE) vulnerability in the component /codebase/dir.php?type=filenew of Mara v7.5 allows attackers to execute arbitrary commands via a crafted PHP file.	2021-10-28	not yet calculated	CVE-2021-36547 MISC
monstra -- monstra	A remote code execution (RCE) vulnerability in the component /admin/index.php?id=themes&action=edit_template&filename=blog of Monstra v3.0.4 allows attackers to execute arbitrary commands via a crafted PHP file.	2021-10-28	not yet calculated	CVE-2021-36548 MISC
mymbconnect24 -- mymbconnect24	In mymbCONNECT24, mbCONNECT24 <= 2.9.0 an unauthenticated user can enumerate valid backend users by checking what kind of response the server sends for crafted invalid login attempts.	2021-10-27	not yet calculated	CVE-2021-34580 CONFIRM
nagios -- xi	An issue was discovered in Nagios XI 5.8.5. In the Manage Dashlets section of the Admin panel, an administrator can upload ZIP files. A command injection (within the name of the first file in the archive) allows an attacker to execute system commands.	2021-10-26	not yet calculated	CVE-2021-40345 MISC MISC MISC
nagios -- xi	An issue was discovered in Nagios XI 5.8.5. In the Custom Includes section of the Admin panel, an administrator can upload files with arbitrary extensions as long as the MIME type corresponds to an image. Therefore it is possible to upload a crafted PHP script to achieve remote command execution.	2021-10-26	not yet calculated	CVE-2021-40344 MISC MISC MISC
nagios -- xi	An issue was discovered in Nagios XI 5.8.5. Insecure file permissions on the nagios_unbundler.py file allow the nagios user to elevate their privileges to the root user.	2021-10-26	not yet calculated	CVE-2021-40343 MISC MISC MISC
nexacr017 -- nexacr017	An Improper input validation in execDefaultBrowser method of NEXACRO17 allows a remote attacker to execute arbitrary command on affected systems.	2021-10-26	not yet calculated	CVE-2021-26607 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nginx -- nginx	A security issue was discovered in ingress-nginx where a user that can create or update ingress objects can use the custom snippets feature to obtain all secrets in the cluster.	2021-10-29	not yet calculated	CVE-2021-25742 MLIST CONFIRM
nvidia -- virtual_gpu_manager	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where a string provided by the guest OS may not be properly null terminated. The guest OS or attacker has no ability to push content to the plugin through this vulnerability, which may lead to information disclosure, data tampering, unauthorized code execution, and denial of service.	2021-10-29	not yet calculated	CVE-2021-1120 CONFIRM
nvidia -- virtual_gpu_manager	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where it can dereference a NULL pointer, which may lead to denial of service.	2021-10-29	not yet calculated	CVE-2021-1122 CONFIRM
nvidia -- virtual_gpu_manager	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where there is the potential to execute privileged operations by the guest OS, which may lead to information disclosure, data tampering, escalation of privileges, and denial of service	2021-10-29	not yet calculated	CVE-2021-1118 CONFIRM
nvidia -- virtual_gpu_manager	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where it can double-free a pointer, which may lead to denial of service. This flaw may result in a write-what-where condition, allowing an attacker to execute arbitrary code impacting integrity and availability.	2021-10-29	not yet calculated	CVE-2021-1119 CONFIRM
nvidia -- virtual_gpu_manager	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager kernel driver, where a vGPU can cause resource starvation among other vGPUs hosted on the same GPU, which may lead to denial of service.	2021-10-29	not yet calculated	CVE-2021-1121 CONFIRM
nvidia -- virtual_gpu_manager	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where it can deadlock, which may lead to denial of service.	2021-10-29	not yet calculated	CVE-2021-1123 CONFIRM
oretnom23 -- pharmacy_point_of_sale_system	An SQL Injection vulnerabilty exists in the oretnom23 Pharmacy Point of Sale System 1.0 in the login function in actions.php.	2021-10-29	not yet calculated	CVE-2021-41676 MISC
phpgurukul -- news_portal_project	SQL Injection vulnerabilities exist in https://phpgurukul.com News Portal Project 3.1 via the (1) category, (2) subcategory, (3) sucatdescription, and (4) username parameters, the server response is about (N) seconds delay respectively which mean it is vulnerable to MySQL Blind (Time Based). An attacker can use sqlmap to further the exploitation for extracting sensitive information from the database.	2021-10-27	not yet calculated	CVE-2021-37808 MISC
phpgurukul -- online_shopping_portal	An SQL Injection vulneraility exists in https://phpgurukul.com Online Shopping Portal 3.1 via the email parameter on the /check_availability.php endpoint that serves as a checker whether a new user's email is already exist within the database.	2021-10-27	not yet calculated	CVE-2021-37807 MISC
portainer -- portainer	An Incorrect Access Control issue exists in all versions of Portainer.via an unauthorized access vulnerability. The vulnerability is also CNVD-2021-49547	2021-10-29	not yet calculated	CVE-2021-41748 MISC
portainer -- portainer	An unauthorized access vulnerabiitly exists in all versions of Portainer, which could let a malicious user obtain sensitive information.	2021-10-29	not yet calculated	CVE-2021-41874 MISC
ranko -- ranko	A vulnerability was discovered in the filename parameter in pathindex.php?r=cms-backend/attachment/delete&sub=&filename=../../../../111.txt&filetype=image/jpeg of the master version of RKCMS. This vulnerability allows for an attacker to perform a directory traversal via a crafted .txt file.	2021-10-29	not yet calculated	CVE-2020-25881 MISC MISC MISC
roblox-purchasing-hub -- roblox-purchasing-hub	Roblox-Purchasing-Hub is an open source Roblox product purchasing hub. A security risk in versions 1.0.1 and prior allowed people who have someone's API URL to get product files without an API key. This issue is fixed in version 1.0.2. As a workaround, add `@require_apikey` in `BOT/lib/cogs/website.py` under the route for `/v1/products`.	2021-10-27	not yet calculated	CVE-2021-41191 MISC CONFIRM MISC
skyworth -- digital_technology_penguin_aurora_box	Skyworth Digital Technology Penguin Aurora Box 41502 has a denial of service vulnerability, which can be exploited by attackers to cause a denial of service.	2021-10-27	not yet calculated	CVE-2021-41872 MISC
sophos -- sophos	A local attacker could bypass the app password using a race condition in Sophos Secure Workspace for Android before version 9.7.3115.	2021-10-30	not yet calculated	CVE-2021-36808 CONFIRM
sorececodster -- online_covid_vaccination_scheduler_system	An SQL Injection vulnerability exists in Sourcecodester Online Covid Vaccination Scheduler System 1.0 via the username in lognin.php .	2021-10-27	not yet calculated	CVE-2021-37803 MISC
sorececodster -- vehicle_parking_managemenr_system	A Stored Cross Site Scripting (XSS) vunerability exists in Sourcecodeste Vehicle Parking Management System affected version 1.0 is via the add-vehicle.php endpoint.	2021-10-27	not yet calculated	CVE-2021-37805 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sorececodster -- vehicle_parking_management_system	An SQL Injection vulnerability exists in https://phpgurukul.com Vehicle Parking Management System affected version 1.0. The system is vulnerable to time-based SQL injection on multiple endpoints. Based on the SLEEP(N) function payload that will sleep for a number of seconds used on the (1) editid , (2) viewid, and (3) catename parameters, the server response is about (N) seconds delay respectively which mean it is vulnerable to MySQL Blind (Time Based). An attacker can use sqlmap to further the exploitation for extracting sensitive information from the database.	2021-10-27	not yet calculated	CVE-2021-37806 MISC
sourcecodester -- budget_and_expense_tracker_system	Remote Code Execution (RCE) vulnerability exists in Sourcecodester Budget and Expense Tracker System 1.0 that allows a remote malicious user to inject arbitrary code via the image upload field. .	2021-10-29	not yet calculated	CVE-2021-41645 MISC
sourcecodester -- church_management_system	Remote Code Execution (RCE) vulnerability exists in Sourcecodester Church Management System 1.0 via the image upload field.	2021-10-29	not yet calculated	CVE-2021-41643 MISC
sourcecodester -- e-negosyo_system	A Remote Code Execution (RCE) vulnerabilty exists in Sourcecodester E-Negosyo System 1.0 in /admin/produts/controller.php via the doInsert function, which validates images with getImageSizei. .	2021-10-29	not yet calculated	CVE-2021-41675 MISC
sourcecodester -- e-negosyo_system	An SQL Injection vulnerability exists in Sourcecodester E-Negosyo System 1.0 via the user_email parameter in /admin/login.php.	2021-10-29	not yet calculated	CVE-2021-41674 MISC
sourcecodester -- online_food_ordering_system	Remote Code Exection (RCE) vulnerability exists in Sourcecodester Online Food Ordering System 2.0 via a maliciously crafted PHP file that bypasses the image upload filters.	2021-10-29	not yet calculated	CVE-2021-41644 MISC
sourcecodester -- online_reviewer_system	Remote Code Execution (RCE) vulnerability exists in Sourcecodester Online Reviewer System 1.0 by uploading a maliciously crafted PHP file that bypasses the image upload filters..	2021-10-29	not yet calculated	CVE-2021-41646 MISC
spring -- spring	In Spring Framework versions 5.3.0 - 5.3.10, 5.2.0 - 5.2.17, and older unsupported versions, it is possible for a user to provide malicious input to cause the insertion of additional log entries.	2021-10-28	not yet calculated	CVE-2021-22096 MISC
spring -- spring	In Spring AMQP versions 2.2.0 - 2.2.18 and 2.3.0 - 2.3.10, the Spring AMQP Message object, in its toString() method, will deserialize a body for a message with content type application/x-java-serialized-object. It is possible to construct a malicious java.util.Dictionary object that can cause 100% CPU usage in the application if the toString() method is called.	2021-10-28	not yet calculated	CVE-2021-22097 MISC
spring -- spring	In Spring Data REST versions 3.4.0 - 3.4.13, 3.5.0 - 3.5.5, and older unsupported versions, HTTP resources implemented by custom controllers using a configured base API path and a controller type-level request mapping are additionally exposed under URIs that can potentially be exposed for unauthorized access depending on the Spring Security configuration.	2021-10-28	not yet calculated	CVE-2021-22047 MISC
spring -- spring	In Spring Cloud OpenFeign 3.0.0 to 3.0.4, 2.2.0.RELEASE to 2.2.9.RELEASE, and older unsupported versions, applications using type-level `@RequestMapping`annotations over Feign client interfaces, can be involuntarily exposing endpoints corresponding to `@RequestMapping`-annotated interface methods.	2021-10-28	not yet calculated	CVE-2021-22044 MISC
sysaid -- sysaid	SysAid 20.4.74 allows XSS via the KeepAlive.jsp stamp parameter without any authentication.	2021-10-29	not yet calculated	CVE-2021-31862 MISC MISC
tenda -- ac1200_router	Stack-based buffer overflow in Tenda AC-10U AC1200 Router US_AC10UV1.0RTL_V15.03.06.48_multi_TDE01 allows remote attackers to execute arbitrary code via the timeZone parameter to goform/SetSysTimeCfg.	2021-10-29	not yet calculated	CVE-2020-22079 MISC MISC
tenda -- ac9	Buffer Overflow vulnerability in Tenda AC9 V1.0 through V15.03.05.19(6318), and AC9 V3.0 V15.03.06.42_multi, allows attackers to execute arbitrary code via the index parameter.	2021-10-29	not yet calculated	CVE-2021-31627 MISC MISC
tenda -- ac9	Buffer Overflow vulnerability in Tenda AC9 V1.0 through V15.03.05.19(6318), and AC9 V3.0 V15.03.06.42_multi, allows attackers to execute arbitrary code via the urls parameter.	2021-10-29	not yet calculated	CVE-2021-31624 MISC MISC
tikiwiki -- tikiwiki	TikiWiki v21.4 was discovered to contain a cross-site scripting (XSS) vulnerability in the component tiki-browse_categories.php. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload under the Create category module.	2021-10-28	not yet calculated	CVE-2021-36550 MISC
tikiwiki -- tikiwiki	TikiWiki v21.4 was discovered to contain a cross-site scripting (XSS) vulnerability in the component tiki-calendar.php. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload under the Add Event module.	2021-10-28	not yet calculated	CVE-2021-36551 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
vim -- vim	vim is vulnerable to Heap-based Buffer Overflow	2021-10-27	not yet calculated	CVE-2021-3903 MISC CONFIRM
yonyou -- turbocrm	SQL Injection vulnerability exists in all versions of Yonyou TurboCRM.via the orgcode parameter in changepswd.php. Attackers can use the vulnerabilities to obtain sensitive database information.	2021-10-29	not yet calculated	CVE-2021-41746 MISC MISC
zoom -- call_recording	Zoom Call Recording 6.3.1 from ZOOM International is vulnerable to Java Deserialization attacks targeting the inbuilt RMI service. A remote unauthenticated attacker can exploit this vulnerability by sending crafted RMI requests to execute arbitrary code on the target host.	2021-10-28	not yet calculated	CVE-2019-19810 MISC MISC

Back to top

This product is provided subject to this Notification and this Privacy & Use policy.